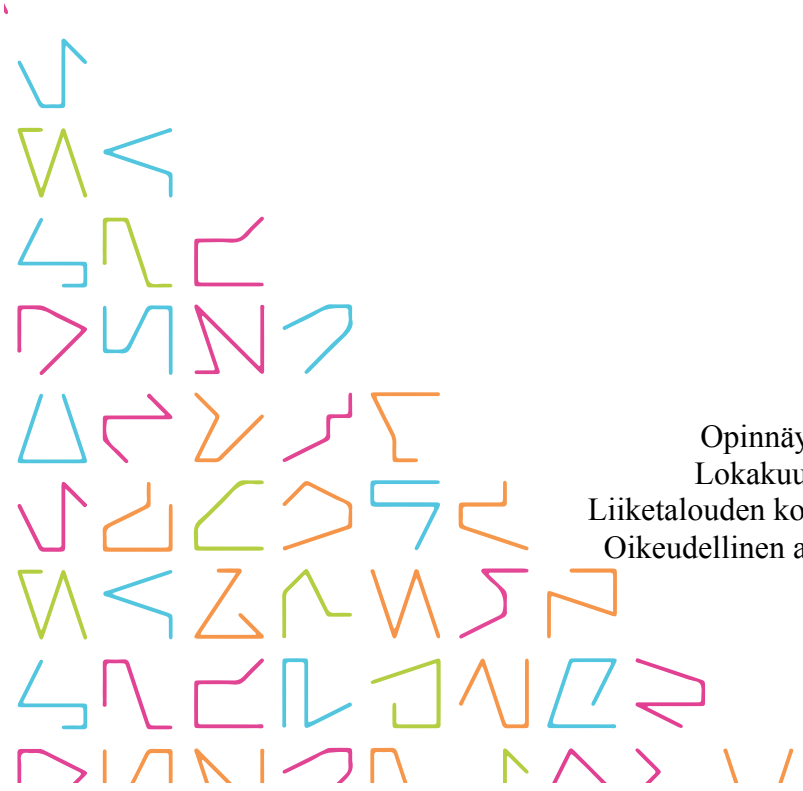
TAMPEREEN
AMMATTIKORKEAKOULU

HENKILÖTIETOJEN TURVALLISEN KÄSITTELYN TOTEUTUMINEN EU:N TIETOSUOJA-ASETUKSEN VAATIMUSTEN MUKAISESTI

Petri Hakonen



Opinnäytetyö
Lokakuu 2017
Liiketalouden koulutusohjelma
Oikeudellinen asiantuntijuus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden koulutusohjelma
Oikeudellinen asiantuntijuus

PETRI HAKONEN
Henkilötietojen turvallisen käsittelyn toteutuminen EU:n tietosuoja-asetusten vaatimusten mukaisesti

Opinnäytetyö 48 sivua, joista liitteitä 0 sivua
Lokakuu 2017

Tässä opinnäytetyössä tutkitaan henkilötietojen turvallisen käsittelyn toteutumista uuden EU:n tietosuoja-asetuksen vaatimusten mukaisesti. Työssä käydään läpi voimassa olevaa lainsäädäntöä ja miten se ohjaa tietosuojaa ja tietoturvaa ja mitä muutoksia kesällä 2018 voimaan tuleva EU:n tietosuoja-asetus tuo tullessaan. Opinnäytetyö keskittyy lähinnä tekniseen ja operatiiviseen tietoturvaan ja selvittää minkälaisia vaatimuksia nykyinen ja tuleva lainsäädäntö edellyttää näiltä osa-alueilta.

Ehdotus uudesta EU:n tietosuoja-asetuksesta annettiin jo vuonna 2012 Euroopan komission toimesta ja se on yksi merkittävimmistä ja eniten kommentoiduista asetuksista. Neljän vuoden aikana komission ehdotukseen kohdistui merkittävää lobbausta ja reilusti yli 4000 muutosehdotusta, joka osoittaa sen tärkeyden eri organisaatioille unionissa. EU:n tietosuoja-asetus hyväksyttiin 14.4.2016 Euroopan neuvoston ja parlamentin päätöksillä. Uusi asetus tulee olemaan merkittävä muutos ja se tulee edellyttämään merkittävän määrän toimenpiteitä varsinkin suuremmilta organisaatioilta.

Työssä tutustutaan myös tietoturva-alaa ohjaaviin kansallisesti ja kansainvälisesti tunnustettuihin standardeihin ja ohjeisiin sekä toimialan hyväksi todettuihin ratkaisuihin ja toimintamalleihin ja miten näiden toteuttaminen auttaa organisaatioita vastaamaan uusien asetusten ja direktiivien vaatimuksiin.

Asiasanat: Euroopan Unioni, tietoturva, tietosuoja, turvallisuus

ABSTRACT

Tampere University of Applied Sciences
Degree Programme in Business Administration
Legal Expertise

PETRI HAKONEN
Realization of the Secure Handling of the Personally Identifiable Data in Compliance with the Requirements of the EU General Data Protection Regulation

Bachelor's thesis 48 pages, appendices 0 pages
October 2017

The purpose of the thesis was to investigate the requirements of the EU general data protection regulation for the secure handling of personally identifiable data. This thesis goes through the existing legislation, how the existing legislation instructs on privacy and information security and what changes will be introduced by the new EU general data protection regulation that will come into in full force in summer 2018. This thesis mainly focuses on the technical and operational information security and what the current and future requirements in this area are.

The initial proposal for the new EU general data protection regulation was introduced by the European Council as early as in 2012, and it has been one of the most significant and commented regulations so far. Within the last four years, major lobbying has been done and over 4000 amendments to the new privacy regulation have been made, which alone shows how important and significant this regulation is for various organisations within the EU. The regulation was approved on 14 April 2016 by the decision of the EU Council and Parliament. The new regulation will be a major change in privacy in the EU and will require a significant number of actions, especially from the larger organisations.

This thesis also introduces the nationally and internationally recognized standards, procedures and the best practises and solutions that guide the information security industry and help organisations to comply with the new regulations and directive requirements.

Keywords: European Union, information security, privacy, security

SISÄLLYS

1 JOHDANTO....7
2 TUTKIMUSAIHE....9
2.1 Tutkimuksenaihe ja metodi....9
2.2 Toimeksiantajan tavoite....9
2.3 Tekijän tavoite....10
3 TIETOSUOJA, KANSALLINEN SÄÄNTELY JA EU-ASETUS....11
3.1 Yleisesti tietosuojasta ja sen sääntelystä....11
3.2 Kansallinen sääntely....12
3.2.1 Perustuslaki (PL 1999/731)....12
3.2.2 Henkilötietolaki (HetiL 1999/523)....12
3.2.3 Rikoslaki (RL 39/1889)....13
3.3 EU:n tietosuoja-asetus (EU) 2016/679....14
3.4 Merkittävät muutokset....15
4 TIETOTURVA....18
4.1 Tietoturvan osa-alueet....22
4.2 Tietoturvan hallinta ja operatiivinen tietoturva....23
4.3 Henkilötietojen turvallisuus, EU:n tietosuoja-asetus....26
4.3.1 Artikla 32....26
4.3.2 Artikla 33....35
4.3.3 Artikla 34....36
4.4 Tietoturvallisuuden yleisesti tunnustettuja standardeja....37
4.4.1 ISO/IEC 27000-perhe....38
4.4.2 Katakri....41
4.4.3 VAHTI....42
5 POHDINTA....45
LÄHTEET....47

ERITYISSANASTO

AV	Antivirus
CIA	Confidentiality, Integrity ja Availability
BCP	Business Continuation Plan
DLP	Data Loss Preventation
DRP	Disaster Recovery Plan
EDPB	European Data Protection Board, Euroopan tietosuojaneuvosto
EU	Euroopan Unioni
FIM	File Integrity Monitoring
HetiL	Henkilötietolaki (1999/523)
IAM	Identity and Access Management (identiteetti ja käyttövaltuushallinta
IDS/IPS	Intrusion Detection System / Intrusion Preventation System
IoT	Internet of Things, nykyisin käytetään myös termiä IoE, eli Internet of Everything
ISO	International Organization of Standardization
ISO/IEC 27000	Tietoturvallisuuden hallintajärjestelmät standardi perhe
ISMS	Information Security Management System
IT	Informaatio Teknologia
Katakri	kansallinen turvallisuusauditointikriteeristö
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
PCI - DSS	Payment Card Industry – Data Security Standard
PL	Perustuslaki (1999/731)
Ransomware	Kiristysohjelma
RL	Rikoslaki (39/1889)
SFS	Suomen Standardoimisliitto ry
Sandbox	Tekniikka jossa havainnon tehnyt laite avaa esimerkiksi potentiaalisen haittaohjelman sisältävän tiedoston suojatussa ympäristössä varmistaakseen ohjelman haitallisuuden/haitattomuuden.
SIEM	Security Incident and Event Monitoring

SOC	Security Operations Center
TI	Threat Intelligence
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VMS	Vulnerability Management System (haavoittuvuuksien hallinta)

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on tutustua Euroopan Unionin uuteen tietosuoja-asetukseen, joka astuu voimaan 28.5.2018, sen asettamiin teknologisiin, operatiivisiin ja prosessuaalisiin vaatimuksiin henkilötietojen turvallisen käsittelyn toteutumiseksi. Työssäni myös verrataan uutta asetusta nykyiseen kotimaiseen lainsäädäntöön ja sen tuomiin merkittävimpiin muutoksiin ja suomalaisten yritysten valmiuteen toimia uuden asetuksen edellyttämällä tavalla.

Nykyaikainen tietotekniikka on mahdollistanut erittäin suurten tietomäärien keräämisen, varastoimisen ja käsittelyn. Yritykset, yhteisöt ja jopa yksityiset kuluttajat ovat riippuvaisia tietotekniikasta ja voidaankin jo todeta koko yhteiskunnan olevan rakennettu tietotekniikan varaan. Tiedon siirtyessä täysin digitaaliseen maailmaan on myös sen ympärillä toimiva rikollisuus monimuotoistunut ja kasvanut räjähdysmäisesti. Vaikka myös turvallisuusteknologia ja järjestelmät ovat kehittyneet, niin niiden käyttöönotto on jäänyt muiden prioriteettien jalkoihin. Tämä on ehkä siksi, että organisaatioissa ei ymmärretä riippuvuutta tietotekniikasta eikä ymmärretä tai mielletä kerätyn tiedon olevan joko suojaamisen tai varastamisen arvoista. Kuitenkin useat tutkimukset osoittavat, että hyökkäykset eri organisaatioita kohtaan ovat päivittäistä arkea ja kukaan ei ole suljettu hyökkäysten kohteiden ulkopuolelle toimialansa tai sijaintinsa takia. Vuosien 2004 - 2014 välillä pelkästään EU:n alueella tapahtui 229 tietovuotoa ja näissä vaarantui yli 200 miljoonan kansalaisen henkilötiedot ja tämä luku pitää sisällään vain tunnetut tietovuodot[1].

Tietosuoja on yksi osa tietoturvaa ja ilman hyvää tietoturvaa ei ole yhdelläkään organisaatiolla riittäviä edellytyksiä suojata hallussaan olevaa tietoa. Tosin on kuitenkin todettava, että hyväkään tietoturva ei täysin suojaa tietämättömyydeltä tai osaamattomuudelta. Tietoturvallisuus jaetaan perinteisesti kahdeksaan (8) eri osa-alueeseen: hallinnollinen, fyysinen, laitteisto, ohjelmisto, tietoaineisto, tietoliikenne, henkilöstö sekä käyttöturvallisuus. Tässä opinnäytetyössä keskitytään uuden tietosuoja-asetuksen edellyttämiin teknisiin ja operatiivisiin tietoturvallisuuden osa-alueisiin. EU:n tietosuoja-asetuksessa näihin edellä mainittuihin osa-alueisiin otetaan kantaa artikloissa 32-34. Henkilökohtaisesti

[1] Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe 2004-2014, s.3. Tutkimusta käytetty Tietoviikon suomen kielisessä artikkelissa 16.10.2014.

koen tämän uuden tietosuoja-asetuksen ongelmalliseksi siinä suhteessa, että se ei määrittele riittävän tarkasti teknisiä vaatimuksia. Kuitenkin tietosuoja-asetuksen mukaiset sanktiot ja niiden antaminen perustuvat merkittävästi siihen onko esimerkiksi tietomurron kohteeksi joutunut organisaatio suojannut tietonsa riittävällä tavalla. Mikä sitten on riittävä taso ja kuka sen määrittelee? Tietoturva-alaa ohjaavat muutamat globaalisti tunnustetut standardit kuten ISO/IEC 27000-perhe, PCI DSS, NIST 800-53 sekä kotimaassa valtionhallinnon KATAKRI ja VAHTI-ohjeistus. Nämä standardit ottavat myös kantaa tietoturvan teknisiin osa-alueisiin ja edellytyksiin hyvälle tietoturvalle. Työssäni olen käyttänyt näitä standardeja määritelläkseni ja selventääkseni minkälaisia teknisiä ja operatiivisia tietoturvajärjestelmiä ja prosesseja pitää organisaatioilla olla paikallaan, jotta EU:n tietosuoja-asetuksen vaatimukset tulevat täytetyksi.

2 TUTKIMUSAIHE

2.1 Tutkimuksenaihe ja metodi

Tässä opinnäytetyössä tutkimuksen kohteena on EU:n tietosuoja-asetus ja sen määrittelemä tietoturvallisuuden taso ja vaatimukset henkilötietojen turvalliselle käsittelylle. Tutkielman tavoitteena on tutustuttaa EU:n tietosuoja-asetukseen ja erityisesti sen artikloiden 32-34 määritelmiin, sekä alan tunnustettuihin standardeihin kuten ISO/IEC 27000-standardiperhe sekä kotimainen VAHTI-ohjeistus ja Katakri. Tutkielmassa keskitytään erityisesti EU:n tietosuoja-asetuksen määrityksiin tekniselle tietoturvallisuudelle, miltä hyvä tekninen ja operatiivinen tietoturva näyttää ja mitkä ovat merkittävimmät muutokset nykyiseen lainsäädäntöön.

Tutkielman tutkimusmetodina on lähinnä lainopillinen eli oikeusdogmaattinen. Oikeusdogmatiikka tutkii voimassa olevien lakien sisältöä ja sen tehtävänä on tulkita ja systematisoida oikeusnormeja. Oikeussääntöjen ohella lainoppi tutkii nykyään myös oikeusperiaatteita ja sen tehtävänä onkin myös punnita niiden yhteensovittamista. Lainoppia voidaankin luonnehtia tulkintatieteeksi[2].

2.2 Toimeksiantajan tavoite

Opinnäytetyön toimeksiantajana on Oy Dell Ab ja heidän tavoitteena toimeksiannolle oli saada Suomen maaorganisaation myyntihenkilöstölle työkaluja asiakkaiden kanssa käytäviin keskusteluihin. Uusi tietosuoja-asetus tulee vaikuttamaan jokaiseen organisaatioon, mutta vaikutusten määrä tulee vaihtelemaan johtuen esikerkiksi organisaation ydintoiminnasta ja koosta. Mahdollisista eritasoisista vaikutuksista huolimatta, tämä uusi asetus ja sen tuomat muutokset ovat ajankohtainen aihe ja hyvä avaus uusille keskusteluille. Itse tutkielman lisäksi tavoitteena on tuottaa koulutuspaketti materiaaleineen, sekä itse koulutustilaisuus, jossa tämä koulutuspaketti käydään läpi Oy Dell Ab:n kohdeyleisölle. Nämä materiaalit ovat erillinen kokonaisuus ja johtuen sen sisältämistä organisaation ainoastaan sisäiseen jakeluun tarkoitetuista tiedoista, se ei ole julkisessa jakelussa ja eikä siten myöskään tämän työn liitteenä.

---

[2] Hirvonen Ari, 2011, s. 36-37

2.3 Tekijän tavoite

Dell Technologies organisaatioon kuuluu useita eri tietoturvaan keskittyneitä yhtiöitä, kuten SecureWorks, jota itse edustan. SecureWorks on yksi maailman johtavista tietoturvapalveluita tarjoavista yhtiöistä ja työllistää globaalisti yli 2000 henkeä ja palvelee yli 4000 asiakasta. Henkilökohtaisena tavoitteena tälle työlle oli löytää aikaa perehtyä uuteen lainsäädäntöön, sen tuomiin muutoksiin ja mahdollisuuksiin. Tämä tieto palvelee päivittäisessä työssäni tietoturvakonsulttina sekä myös urani seuraavalla askeleella. Tietosuojaasetus tulee tarjoamaan merkittäviä liiketoiminnallisia mahdollisuuksia nyt ja tulevaisuudessa kun lainsäädännön kautta luodaan vihdoinkin pakottava tarve organisaatioille ymmärtää tietoturvan tärkeys, ellei jopa pakollisuus turvaamaan liiketoiminnan jatkuvuutta.

3 TIETOSUOJA, KANSALLINEN SÄÄNTELY JA EU-ASETUS

3.1 Yleisesti tietosuojasta ja sen sääntelystä

Perinteisesti termi tietosuoja on liitetty henkilötietolain vaatimuksiin taata yksityisyys, oikeudet ja oikeusturva käsiteltäessä materiaalia, joka sisältää yksityisten henkilöiden tietoja. On voitukin todeta, että tietosuojan periaatteellinen tarkoitus on suojata yksityisen henkilön tai tiedon kohteen yksityisyys, oikeusturva, oikeudet ja vapaudet.[3] Henkilötietojen käsittelyn ja suojaamisen merkitys on kasvanut jo pitkään johtuen palveluiden ja tietojen sähköistymisestä. Tietotekniikan kehittyminen on mahdollistanut suurten tietomäärien keräämisen, tallentamisen sekä hyödyntämisen ja henkilötiedot ovat kuin polttoainetta uusille digitaalisille palveluille[4]. Uudet trendit kuten palvelupohjaiset pilvi-ratkaisut tai IoT (Internet of Things) valtaavat alaa ja nämä uudet toimintatavat tulevat räjähdysmäisesti kasvattamaan kerättävän datan määrän seuraavien 5-10 vuoden aikana, kun verkkoon kytketään miljardeja uusia laitteita[5]. Nämä uudet mahdollisuudet tuovat mukanaan myös uusia ja suurempia riskejä, mikä tulee edellyttämään entistä suurempia ja kattavampia turvatoimia. Tämän kehityksen suunnan on myös Euroopan unioni huomannut ja nyt myös reagoinut uuden sääntelyn kautta[6].

Tähän asti henkilötietojen suojaamisen sääntely on ollut hyvin pirstaleista. Seuraavissa osissa tätä tutkielmaa käsittelen merkittävimpiä lakeja, kuten perustuslaki (PL 1999/731), henkilötietolaki (HetiL 1999/523) sekä rikoslaki (RL 1889/39), jotka tietosuojaa sääntelevät. Näiden lisäksi on suuri määrä muita kansallisia lakeja ja säännöksiä, jotka eri tavoin ottavat kantaa tietosuojaan ja sen toteutumiseen, kuten laki yksityisyyden suojasta työelämässä (759/2004; työelämän tietosuojalaki), sähköisenviestinnäntietosuojalaki (516/2004), laki henkilötietojen käsittelystä poliisitoimessa (761/2003), laki henkilötietojen käsittelystä rajavartiolaitoksessa (579/2005) sekä laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007). Tämä lainsäädännön hajanaisuus on ollut omiaan aiheuttamaan hämmennystä ja epävarmuutta eri lakien ja sääntelyn keskinäisistä suhteista ja eritoten millä viranomaisella on vastuu, velvollisuus ja toimivaltuus

[3] Järvinen Petteri, 2010, Yksityisyys – Turvaa digitaalinen kotirauhasi, s. 15
[4] VAHTI - raportti 1/2016, EU-tietosuojan kokonaisuudistus
[5] VAHTI - Valtionvarainministeriön julkaisuja 25/2017, Sähköisen asioinnin tietoturvallisuusohje. s. 11
[6] CGI Kyberturvallisuus digitalisoituvassa maailmassa, 2016, s. 2-4

kussakin tilanteessa. Kun vastuut, velvollisuudet ja toimivaltuudet eivät ole selkeästi määritelty haittaa se myös digitaalisten palveluiden käyttöön ottoa.

3.2 Kansallinen sääntely

Kuten jo aikaisemmin on todettu, Suomen lainsäädännössä ei ole tietosuojaan tai tietoturvaan keskittyvää spesifistä yleissäädöstä, vaan erilaiset turvallisuussäädökset ovat hajaantuneet useisiin eri säädöksiin, joista merkittävimpinä ovat perustuslaki, henkilötietolaki ja rikoslaki.[7]

3.2.1 Perustuslaki (PL 1999/731)

Perustuslain 10 § ottaa kantaa tietosuojaan, joka käsittelee yksityiselämän suojaa. Sinänsä 10 § on hyvinkin lyhyt ja yksinkertainen, mutta se antaa pohjan jolla määritellään, että jokaisen yksityiselämä, kunnia ja kotirauha on taattu. Tämän lisäksi 10 § määrittelee luottamuksellisen viestin salaisuuden olevan loukkaamaton, oli kyseessä sitten kirje, puhelu tai muunlainen viesti. Laki ei ota kantaa viestintävälineeseen vaan ainoastaan sen tarjoamaan suojaan.

3.2.2 Henkilötietolaki (HetiL 1999/523)

Henkilötietolain edeltäjänä voidaan pitää 1980-luvun lopulla säädettyä henkilörekisterilakia 471/87, jota pidetään Suomen ensimmäisenä tietoturvasäädöksenä. Henkilörekisterilain kumosi nykyinen henkilötietolaki (HetiL 535/1999). Henkilötietolain päätarkoituksena on toteuttaa perusoikeuksia, kuten yksityiselämän suojaa, itsemääräämisoikeutta, vapautta ja turvallisuutta. Henkilötietolaki toteuttaa myös aikaisemmin tässä työssä mainitun perustuslain 10 §:ssä säädetyn velvoitteen säätää henkilötietojen suojasta laintasaisesti.[8] Kun henkilötietolakia tarkastellaan tietoturvan näkökulmasta, niin voidaan todeta, että lain tarkoituksena on myös edistää ja kehittää hyvää tietojenkäsittelytapaa. Laki edellyttää, että henkilötietoja käsitellessä on varmistettava myös hallinnollisen ohjeistuksen ohella, että käsittelyn tekninen toteutus on asianmukainen. Toki on todettava, että myöskään henkilötietolaki ei säädä yksityiskohtaisesti mikä on asianmukainen tekninen toteutus vaan se tyytyy lähinnä tarkastelemaan asiaa suhteellisuusperiaatteen kautta. Laissa

[7] Pitkänen Olli, Tiilikka Päivi, Warma Eija, Henkilötietojen Suoja 2013, s.4-7.
[8] Nyyssölä Mikko, Yksityisyyden suoja työsuhteessa 2014, Lainsäädäntö 3.1

kuten oikeassa elämässäkään ei voida tavoitella absoluuttista turvaa, vaan se pitää suhteuttaa kohteen suojaustarpeeseen. Henkilötietolaki säätää 7 luvussa tietoturvallisuudesta ja tietojen säilytyksestä. HetiL 32.1 §:n mukaan on toteutettava *”tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä”.*[9]

Miten henkilötietolakia sitten Suomessa noudatetaan ja kuinka tuttu se on eri organisaatioille? Tietosuojavaltuutetun toimisto selvitti kotimaisissa verkkopalveluita tarjoavissa tahoissa, kuinka hyvin he ovat huomioineet henkilötietolainsäädännön vaatimukset. Vuonna 2012 suoritettiin tarkastus, joka kohdistettiin organisaatioihin, jotka olivat olleet edeltävänä vuonna tietoturvaloukkauksen tai sen uhan kohteena. Saatujen vastausten perusteella voitiin todeta, että ainoastaan 46 prosentissa kohteena olleista yrityksistä ilmoittivat tuntevansa kyseisen lain vaatimukset tietojen suojaamisen osalta. Tämä luku saattaa tänä päivänä olla jo hieman suurempi, mutta perustuen omaan kokemukseen ei suomalaisissa organisaatioissa olla edelleenkään perehdytty, saati investoitu tähän osa-alueeseen merkittävästi.[10]

3.2.3 Rikoslaki (RL 39/1889)

Sanktiot ovat jo aikaisemmin liittyneet keskeisesti tietosuojalainsäädäntöön, mutta vasta EU:n tietosuoja-asetus tuo ne tarpeeksi merkittävälle tasolle, jotta ne saavat riittävää kunnioitusta organisaatioilta. Nykyisessä lainsäädännössä HetiL 48 § ja RL 38 luvun 9 momentissa on tietoturvasäännösten rikkominen määritelty rikkomukseksi ja tämä on omiaan tuomaan rikoksen ja sen mahdollisten sanktioiden tason alhaiseksi. Uskon että tämän alhaisen tason syynä on, että lakeja säädettäessä ei osattu vielä ottaa huomioon kuinka suureen merkitykseen henkilötiedot tulevat nousemaan verkottuneessa yhteiskunnassa. Rikoslaista löytyy kaksi lukua jotka antavat suojaa yksilön omille tiedoille ja kriminalisoivat mahdolliset rikolliset toimet jotka näitä oikeuksia rikkovat. Rikoslain luku 24 käsittelee aiheita kuten kotirauhan rikkominen, salakuuntelu, kunnianloukkaus ja yksityiselämää loukkaavan tiedon levittäminen. Edellä mainittujen lisäksi luku 38 ottaa kantaa muun muassa salassapitorikokseen, viestintäsalaisuuksien loukkaamiseen, tietomurtoon ja henkilörekisteririkokseen.

---

[9] HetiL 535/1999, 32.2 §
[10] Tietosuojavaltuutetun toimiston lehdistötiedote 10.10.2012.

3.3 EU:n tietosuoja-asetus (EU) 2016/679

Ehdotus uudesta EU:n tietosuoja-asetuksesta (EU) 2016/679 annettiin jo vuonna 2012 Euroopan komission toimesta ja se on yksi merkittävimmistä ja eniten kommentoiduista asetuksista. Neljän vuoden aikana komission ehdotukseen kohdistui merkittävää lobbausta ja reilusti yli 4000 muutosehdotusta, joka osoittaa sen tärkeyden eri organisaatioille unionissa. EU:n tietosuoja-asetus hyväksyttiin 14.4.2016 Euroopan neuvoston ja parlamentin päätöksillä. Uusi asetus tulee olemaan merkittävä muutos ja se tulee edellyttämään merkittävän määrän toimenpiteitä varsinkin suuremmilta organisaatioilta. Tällä hetkellä on käynnissä vielä kahden vuoden siirtymäaika ja uusi tietosuoja-asetus astuu täysin voimaan 25.5.2018. Koska kyseessä on asetus, se asettaa tavoitteet, joihin unionin valtioiden on päästävä. Tätä kautta jokaisessa unionin jäsenmaassa on kansallista henkilötietojen käsittelyä ohjaava lainsäädäntö, eikä jäsenmailta edellytetä erillistä kansallista lainsäädäntötoimia vaan asetus, joka on EU:n sekundäärinormi on suoraan sovellettavissa. Vaikkakin uusi asetus tulee työllistämään suuria globaaleja organisaatioita, se tulee myös tulevaisuudessa helpottamaan tietojen siirtoa, varastointia ja käsittelyä mikä tapahtuu yli rajojen. Tämä siksi, että jokaisessa jäsenmaassa on samat säännöt, joita noudatetaan vanhojen kansallisten lakien sijasta, jotka saattoivat poiketa merkittävästi toisistaan. Vaikkakin asetuksen nimessä mainitaan EU, se ei kosketa ainoastaan EU:n jäsenmaita vaan se koskettaa myös kaikkia muita maita ja organisaatioita, jotka järjestelmissään käsittelevät tai varastoivat EU-kansalaisten tietoja. Asetuksen vaikutus ei siis rajoitu organisaation sijainnin mukaan, vaan tietojen mukaan joita he käsittelevät.

Kuten kansallinen tietosuojaa koskettava lainsäädäntö on myös EU:n nykyinen lainsäädäntö jo aikansa elänyttä. Nykyinen vielä voimassa oleva vuoden 1995 henkilötietodirektiivi (95/46/EY) on ajalta, jolloin henkilötietojen hyödyntäminen ja käsittely liiketoiminnassa oli merkittävästi erilaista ja vähäisempää. Myös toimintaympäristö on tänä päivänä globaalimpi verkottuneisuuden kautta ja uudet palvelut kuten sosiaalinen media, pilvipalvelut, IT-ulkoistukset ja uusin trendi ”digitalisaatio” ovat muuttaneet pelikenttää ja tietosuojan luonnetta. Nykyinen teknologia, sen kehittyminen ja tulevaisuuden näkymät edellyttivät uutta ja tämän päivän haasteisiin vastaavaa lainsäädäntöä, joka tarjoaa teknologia riippumattoman ja riskilähtöisen lainsäädännön.

Kuva 1. EU:n tietosuoja-asetuksen sisältö ja tavoite.[11]

3.4 Merkittävät muutokset

Mitä ovat uuden tietosuoja-asetuksen merkittävimmät muutokset organisaatioille, jotka käsittelevät EU kansalaisten tietoja?

a) Tietosuoja oletukseksi - Privacy by default sekä Privacy by design.
   Artikla 25 löytyy termi ”sisäänrakennettu ja oletusarvoinen tietosuoja” ja tämä artikla määrittelee, miten tietosuoja tulisi ottaa huomioon palvelun koko elinkaaren ajan aina suunnitteluvaiheesta ylläpitoon ja sen alasajoon asti. Jokaisen järjestelmän jossa suojattavia henkilötietoja käsitellään, tulee täyttää asetuksen vaatimukset. Tämän varmistaminen on rekisterinpitäjän vastuulla ja heidän tulee toteuttaa tarvittavat organisatoriset ja tekniset järjestelmät sekä prosessit ja varmistaa että ne ovat paikoillaan. Rekisterinpitäjien vastuulla on myös varmistaa, että oletusarvoisesti kerätään vain toiminnan kannalta välttämättömiä henkilötietoja ja niitä ei kerätä tai säilytetä suurempia määriä tai pidempään kuin on toiminnan kannata tarvittavaa. [12]

[11] EU:n yleinen tietosuoja-asetus. 2017. Verkkodokumentti. OpiTietosuojaa.
[12] VAHTI-raportti, 1/2016. s.22

b) Tietosuojavastaava - Data privacy officer.

Artikla 37 määrittelee vaatimukset, jolloin organisaation tulee nimittää tietosuojavastaava. Jokaisella organisaatiolla jonka keskeisiin toimintoihin kuuluu henkilötietojen käsittelytoimia ja ne vaativat rekisteröityjen järjestelmällistä seurantaa laajassa mittakaavassa, tulee olla nimetty tietosuojavastaava. Huomioitavaa on se, että asetus ei ota kantaa organisaation kokoon tai toimialaan vaan ainoastaan toiminteisiin ja mittakaavaan. Tietosuojavastaavan merkittävimpiin velvollisuuksiin tulee myös kuulumaan kehittämissuunnitelmien teko, toteutus ja valvonta sekä asiantuntija avun tarjoaminen organisaation johdolle sekä muulle henkilöstölle.[13] On myös huomioitava, että mikäli organisaation henkilöstössä ei ole tarvittavaa osaamista ja kokemusta, voidaan tietosuojavastaava hankkia esimerkiksi palveluna niitä tarjoavilta tahoilta.[14]

c) Lasten henkilötietojen rekisteröinti - Age of Consent

Asetuksen artikla 8 rajoittaa tietoyhteiskunnan palveluiden tarjoamisen suoraan lapsille ilman vanhempien suostumusta. Ikäraja on asetettu 16:sta ikävuoteen ja siten esimerkiksi sosiaalisen median palveluiden käyttö vaatisi alle 16-vuotiaalta vanhempien suostumuksen. Jäsenvaltio voi päättää myös alemmasta ikärajasta ja alimmillaan se voi olla 13 vuotta.

d) Ilmoitus tietojen vuotamisesta - Data breach notification

Artikla 33 edellyttää, että mikäli organisaatiossa tapahtuu tietomurto/tietoturvaloukkaus jossa vaarantuu henkilötietoja, on rekisterinpitäjän ilmoitettava siitä ilman viivästystä ja mahdollisuuksien mukaan 72 tunnin sisällä valvontaviranomaiselle. Mikäli ilmoitus myöhästyy, on mukaan liitettävä selvitys viivästyksen syistä.

e) Oikeus tulla unohdetuksi - Right to be forgotten, Right to data portability

Artikla 17 kuvaa hyvin yksinkertaisesti rekisteröidyn oikeuden tietojensa poistamiseksi tai tullakseen unohdetuksi. Artiklan lähtökohta on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskettavat tiedot ilman viivytystä. Tämä ei ole kuitenkaan täysin automaattista vaan tiettyjä perusteita vaatimukselle täytyy olla. Näitä perusteita ovat esimerkiksi:

---

[13] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Artikla 37
[14] VAHTI-raportti, 1/2016. s.18-19

1. Henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin.
2. Rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut.
3. Henkilötietoja on käsitelty lainvastaisesti.

Peruslähtökohtana asetuksessa on kuitenkin, että kun tietoja ei enää tarvita ja niiden säilyttämiselle ja käsittelylle ei ole perustetta, ne tulee hävittää.

f) Hallinnolliset seuraamukset - Administrative sanctions

Artikla 83 määrittelee edellytykset mielestäni asetuksen merkittävimmälle muutokselle eli hallinnollisille sakoille. Uusi asetus tuo mukanaan mahdollisesti todella merkittävät seuraamukset velvoitteitansa laiminlyöville organisaatioille. Mahdolliset asetuksen vastaiset sanktioivat teot on jaettu kolmeen eri luokkaan, joissa hallinnollisen sakon määrä vaihtelee 10 – 20 miljoonan euron välillä. Näiden lisäksi sakko voidaan määrätä sidottavaksi organisaation kokonaisliikevaihtoon ja tällöin käytettävä sakon prosenttiluku on neljä. Seuraamuksiin voidaan kuitenkin liittää myös artiklassa 33 mainittu pakollinen ilmoitus. Tällä on merkittävä taloudellinen vaikutus, kun puhutaan maineriskistä ja sen mahdollisesti tuomasta suorasta vaikutuksesta liiketoimintaan. Hallinnollisista sakoista ja asetusta soveltavista päätöksistä vastaa Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB).

4 TIETOTURVA

Nykyaikainen teknologia mahdollistaa aivan uusia tapoja tehdä liiketoimintaa, innovoida, tavoittaa laajempia markkinoita ja tehdä kaiken tämän nopeammin ja tehokkaammin kuin ennen. Tämä kehitys tuo tietysti hyötyjä näitä tuotteita ja palveluita toteuttaville organisaatioille, mutta myös kuluttajille ja koko yhteiskunnalle. Vaikkakin uusi teknologia mahdollistaa näitä positiivisia asioita tuo se mukanaan myös uusia ja merkittäviä haasteita. Organisaatioiden täytyy muuttua ja kehittyä tekniikan mukana, investoida osaamiseen ja teknologiaan sekä päivittää prosessejaan ja toimintamallejaan vastaamaan näihin teknologisiin edistysaskeleisiin. Monessa organisaatiossa sukelletaan sokeana eteenpäin ilman todellista ymmärrystä näiden teknologisten edistysten mahdollisista vaikutuksista, niiden tuomista mahdollisuuksista, mutta myös mukana tulevista uusista riskeistä. [15]

Uusien teknologisten ratkaisuiden käyttöönotto ja sen aiheuttama suurempi kontaktipinta julkiseen verkkoon, ovat lisänneet merkittävästi organisaatioiden riskejä joutua erilaisten verkkohyökkäyksien kohteeksi ja näitä hyökkäyksiä nykyään käsitelläänkin mediassa lähes päivittäin. Verkkorikollisuus onkin nykyään yksi nopeimmin kasvavista liiketoiminta-alueista. Lain vastaista kyllä, mutta rikollisille erittäin tuottavaa liiketoimintaa, johon pääsee käsiksi hyvinkin pienillä investoinneilla. Rikollisorganisaatioiden lisäksi mukaan joudutaan laskemaan valtiolliset toimijat ja kilpailijat, jotka yrittävät hankkia omaa organisaatiota kiinnostavaa tietoa saadakseen edun puolelleen. Uhkat eivät ole yksistään ulkoisia, vaan organisaatioiden pitää pystyä havaitsemaan ja vastaamaan myös sisäisiin uhkiin, joita aiheuttavat esimerkiksi pettyneet työntekijät ja yleisesti vain tietämättömyys, varomattomuus ja huolimattomuus sekä niistä seuranneet tietovuodot. [16] Organisaatioihin kohdistuvat uhat ovat moninaisia ja monimutkaisia ja siksi tietoturvan pitäisi olla korkeassa asemassa organisaatioiden asialistalla. Nämä uhkat kohdistuvat kaikkiin organisaatioihin ottamatta kantaa organisaation toimialaan tai kokoon eli jokaisella organisaatiolla tulisi olla kyky tunnistaa heihin kohdistuvat riskit, kyky havaita mahdolliset hyökkäykset sekä kyky puolustautua minimoidakseen vahingot. [17]

---

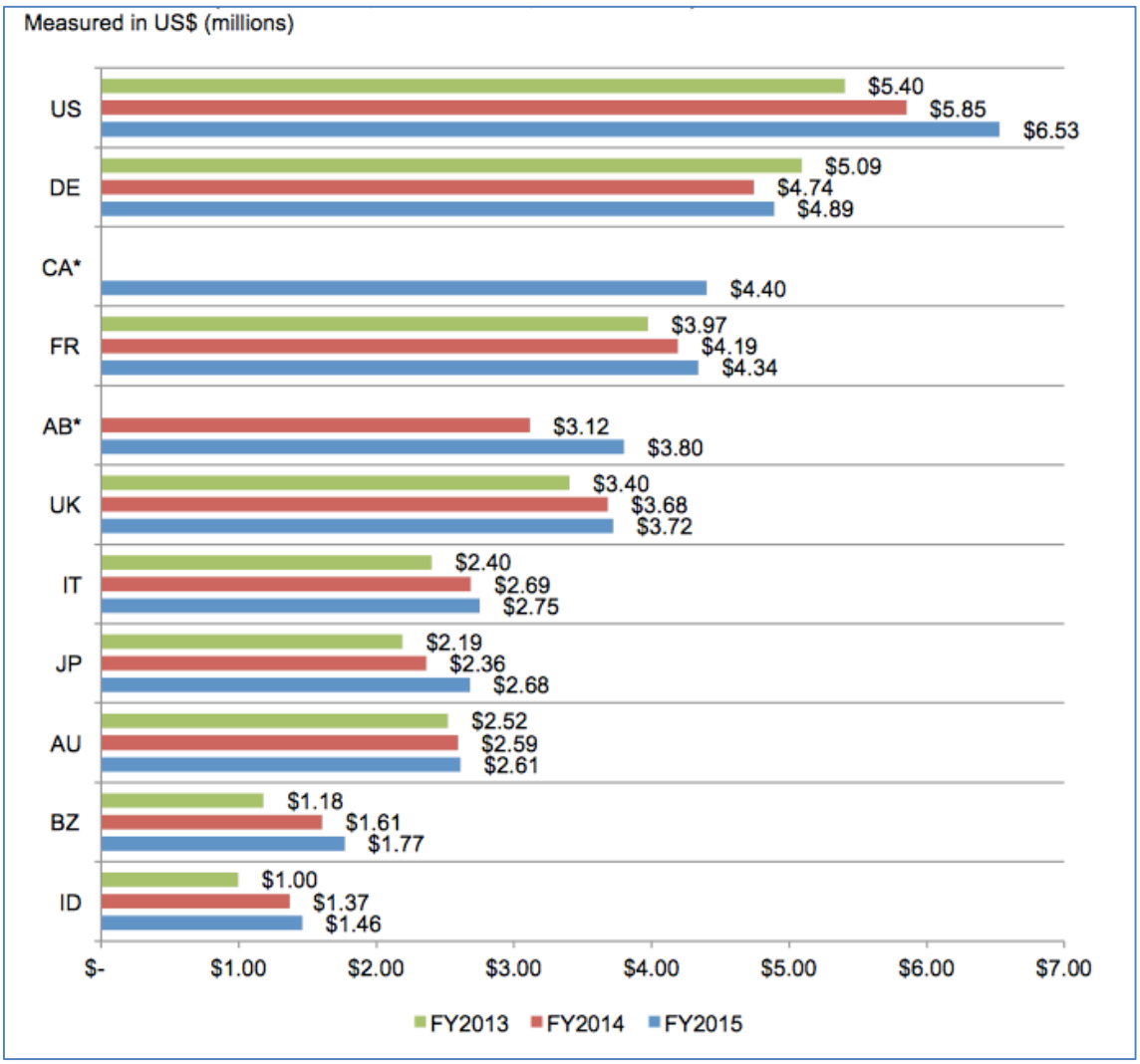
[15] CGI Kyberturvallisuus digitalisoituvassa maailmassa, 2016, s. 4
[16] ICC Cyber security guide for business 2015, s. 4
[17] Andreasson Ari, Koivisto Juha, 2013, Tietoturvaa Toteuttamassa, s. 32-33

Viimeisten vuosien aikana on tietoturvaloukkausten ja tietoturvapoikkeamien määrä moninkertaistunut ja julkisuudessa onkin nähty uutisointia liittyen merkittäviin tietomurtoihin. Viestintävirasto kertoi tietoturvan vuoden 2016 julkaisussaan suomalaiseen infrastruktuuriin kohdistuvista häiriöstä ja uhkista, jotka ovat hyviä konkreettisia esimerkkejä siitä, miten huomattavia vaikutuksia laajalla verkkohyökkäyksellä voisi olla koko yhteiskuntaan. Alkuvuodesta 2016 koettiin kaksi laajaa ja pitkäkestoista häiriötä matkapuhelinverkoissa. Sinänsä, ei kuullosta vakavalta, mutta kun ajatellaan faktaa, että jotkin organisaatiot ovat rakentaneet esimerkiksi ihmishengen kannalta kriittisiä palveluitaan matkapuhelinverkon varaan laittaa se tapahtuneen eri perspektiiviin. Toinen kriittiseen infrastruktuuriin kohdistunut häiriö oli Lappeenrannassa lämmönsyöttöä ohjanneisiin laitteisiin kohdistunut verkkohyökkäys. Hyökkäyksestä aiheutunut lämmönsyötön häiriö kylmensi useita asuntoja alueella. Mikä tekee tästä esimerkistä mielenkiintoisen, on se, että nämä automaatiojärjestelmät eivät olleet hyökkääjän varsinainen kiinnostuksen kohde, vaan ne olivat huonosti suojattu ja siten helposti hyödynnettävissä oleva väline Suomen ulkopuolelle kohdistuneeseen hyökkäykseen. Vaikkakin varsinainen hyökkäys ei kohdistunutkaan meihin, niin vaikutukset kuitenkin konkreettisesti koimme. [18] Edellä mainittujen kotimaisten tapausten lisäksi voidaan viime vuosilta listata Bangladeshilaiseen pankkiin kohdistunut hyökkäys, joka on myös historian suurin pankkiryöstö, jossa hyökkääjien mukaan lähti arviolta 81 miljoonaa dollaria sekä Yahoon tietovuoto, joka taas vastaavasti on historian suurin tietovuoto, jossa hakkereiden mukana lähtivät yli 500 miljoonan käyttäjän tiedot.

Mitä ovat tietoturvaloukkausten seuraukset organisaatioille? Vaikutukset ovat moninaisia ja ne kattavat suoran vaikutuksen varallisuuteen, kuten Bangladeshilaisen pankin tapauksessa, mutta myös organisaation maine, suhteet ja yrityssalaisuudet ovat vaarassa. Maineelle ja suhteille tapahtuneelle vaikutukselle on vaikea laskea suoraan rahallista arvoa, vaan se näkyy vasta pidemmän ajan kuluttua. Yksi syy myös arvioiden puuttumiselle on se, että läheskään kaikki tietomurrot eivät ole julkisessa tiedossa, mutta tähän uusi EU asetus tuo muutoksen velvoitteillaan. Ponemon instituutti ja CGI ovat viime vuosina tutkimuksissaan kartoittaneet tietomurtojen rahallista vaikutusta organisaatioille ja vaikutuksia voidaan pitää merkittävinä. Suuryrityksille yksittäisten hyökkäysten aiheuttamat kustannukset ovat olleet jopa satoja miljoonia dollareita. Esimerkiksi Iso-Britanniassa 81

[18] Viestintäviraston julkaisu 001/2017 J, Tietoturvan vuosi 2016, s. 2

prosenttia suurista organisaatioista oli joutunut vuoden 2016 aikana tietoturvaloukkauksen kohteeksi ja loukkauksista aiheutuneet kustannukset kaksinkertaistuivat vuoden 2016 aikana 0,6–1,15 miljoonan punnan suuruisiksi per organisaatio. Toisena esimerkkinä voidaan käyttää kahden Yhdysvaltalaisen kauppaketjun maksukorttirekisteriin tehtyjä tietomurtoja. Näistä tietomurroista on tähän päivään mennessä aiheutunut näille kahdelle Yhdysvaltalais yritykselle noin 252 miljoonan dollarin suorat vahingot. Toki tästä 252 miljoonan dollarin summasta on korvattu vakuutuksin noin 90 miljoonaa dollaria. Näiden edellä mainittujen vahinkojen lisäksi on näillä kahdella kauppaketjulla vielä kesken oikeusprosessit näistä tietomurroista, joissa vaaditaan noin 200 miljoonan dollarin korvausvaatimuksia [19].



Kuva 2. Ponemon institute, The average total organizational cost of a data breach over three years[20]

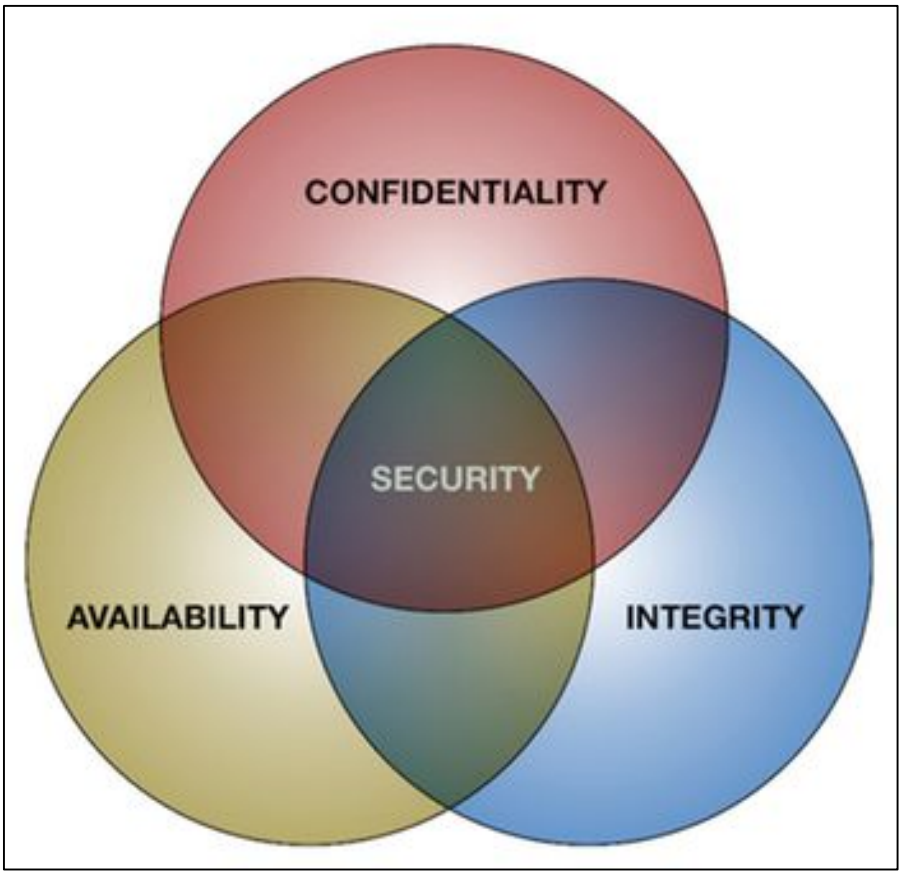
[19] Liikenne ja viestintäministeriö, Julkaisuja 4/2016, s. 17
[20] Ponemon Institute, Cost of Data Breach Study, 2015, s. 7

Kaikki huomio tietomurtojen ympärillä ja uusi tiukempi lainsäädäntö luulisi herättäneen myös organisaatioiden huomion ja kiinnostuksen omasta tietoturvan tasosta. Valitettavasti vielä vuosien 2015-2016 aikana tehdyissä tutkimuksista tätä kehitystä ei vielä ole näkyvissä, vaan merkittävä osa yrityksistä lähes toimialasta riippumatta eivät ole pitäneet edes tarpeellisena, että organisaatiossa olisi tietoturvasta vastaava henkilö, saati sitten toimeen keskittynyt organisaatio[21] [22].

Kuva 3. CGI Kyberturvallisuuden tila suomalaisissa organisaatioissa, 2016 [23]

Mitä sitten tarkoitetaan tietoturvalla ja mitä se pitää sisällään? Tietoturva tai tietoturvallisuus tarkoittaa tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamista. Tämä tietoturvan kolminaisuus tunnetaan toimialalla, myös lyhenteellä CIA, Confidentiality, Integrity ja Availability. Näihin kolmeen useasti vielä lisätään termit kiistämättömyys, tunnistus ja todennus [24] [25].

[21] CGI Kyberturvallisuuden tila suomalaisissa organisaatioissa, 2016, s. 4
[22] Ponemon Institute, Cost of Data Breach Study, 2015, s. 1-2
[23] CGI Kyberturvallisuuden tila suomalaisissa organisaatioissa, 2016, s. 4
[24] National Institute of Standards and Technology, 2001, NIST Special Publication 800-33, s. 2
[25] Järvinen Petteri, 2010, Yksityisyys – Turvaa digitaalinen kotirauhasi, s. 15



Kuva 4. Tietoturvan kolme ulottuvuutta (mukaillen NIST 800-33).

4.1 Tietoturvan osa-alueet

Tietoturvallisuudessa ei ole kysymys vain tiedon suojaamisesta sen digitaalisessa muodossa, vaan se on laajempi käsite, joka kattaa tiedon suojaamisen sen kaikissa olomuodoissa. Perinteisesti tietoturvallisuus on jaettu kahdeksaan eri osa-alueeseen[26] [27]:

1. *”Hallinnollinen tietoturva: hallinnollinen tietoturva kattaa ne toimenpiteet, joilla määrätään organisaatiossa noudatettavat periaatteet ja toimintalinjat: turva-, toipumis- ja valmiussuunnitelmat.*
2. *Fyysinen tietoturva: sisältyy laitteisto-, käyttö- ja varastointitilojen, arkistojen sekä laitteiden ja materiaalien fyysinen suojaus sekä tietoverkon kaapeloinnin suojaus.*
3. *Laitteistoturvallisuus: kuuluu laitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvät turvallisuusominaisuudet.*

[26] Karvi, Tietojenkäsittelylaitos, Helsingin Yliopisto, 2011, Tietoturvan perusteet, s. 4-5
[27] Andreasson Ari, Koivisto Juha, 2013, Tietoturvaa Toteuttamassa, s. 52

4. *Ohjelmistoturvallisuus: kuuluu käyttöjärjestelmien, sovellusohjelmien ja tietoliikenneohjelmistojen turvallisuusominaisuudet.*
5. *Tietoaineiston turvallisuus: sisältää asiakirjojen, tietueiden ja tiedostojen tunnistamisen ja turvallisuusluokituksen sekä tietovälineiden hallinnan ja säilytyksen kaikissa eri käsittelyvaiheissa luomisesta hävittämiseen saakka.*
6. *Tietoliikenneturvallisuus: kattaa ne toimenpiteet, joilla pyritään varmistamaan tietoverkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys.*
7. *Henkilöstöturvallisuus: kattaa henkilöstöön liittyvien luotettavuusriskien hallinnan toimenkuvien, käyttöoikeuksien määrittelyjen sekä turvallisuuskoulutuksen ja valvonnan avulla.*
8. *Käyttöturvallisuus: kuuluu henkilöstön turvalliset käyttöperiaatteet, käyttöympäristöön ja varsinaisen tietojenkäsittelyn turvallisuuteen vaikuttavien tapahtumien valvonta sekä jatkuvuuden turvaamiseen liittyvien menettelyjen käyttö"* [28].

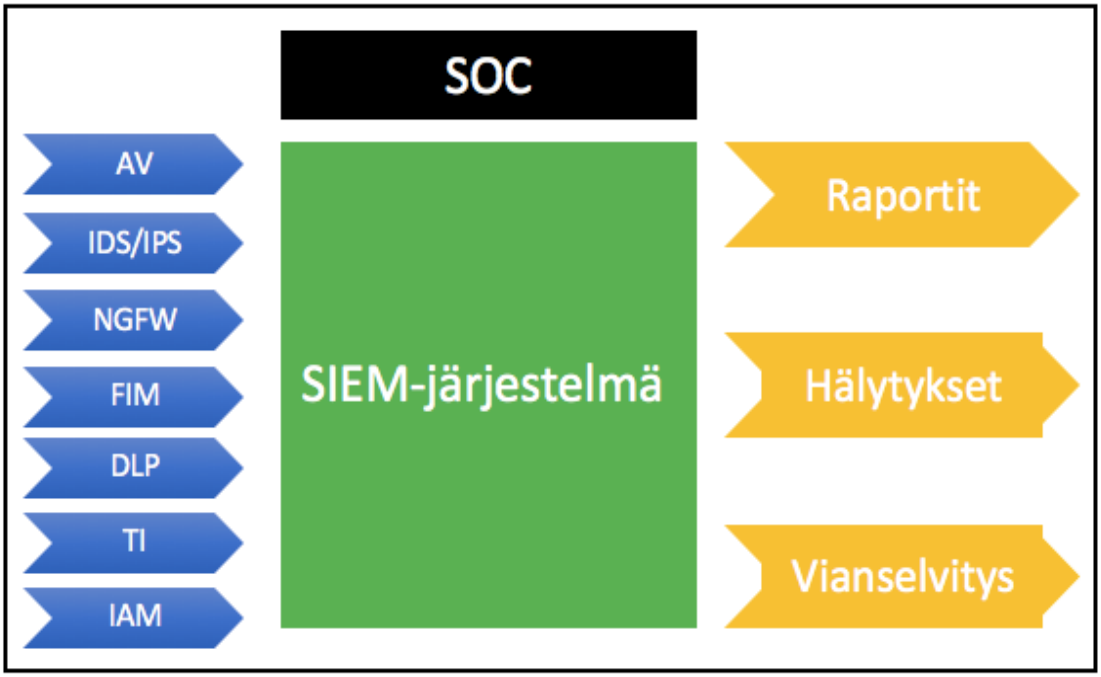
4.2 Tietoturvan hallinta ja operatiivinen tietoturva

Organisaation tietoturvan keskiössä ovat tietoturvan hallinta ja operatiivinen tietoturva. Tietoturvatyö pitää sisällään prosesseja ja kontrolleja, joilla varmistetaan organisaation toiminnan jatkuminen ja laatu tietoturvallisuuden näkökohdista. Mikäli näitä prosesseja ja kontrolleja ei monitoroida, arvioida ja ajoittain tarkisteta, niin mistä voidaan tietää niiden oikeellisuus ja toimivuus. Tietoturvan hallintajärjestelmän tarkoitus on systematisoida ja helpottaa tietoturvallisuustyön johtamista, kehittämistä, auttaa reagoimaan muuttuvaan toimintaympäristöön sekä varmistamaan, että valitut kontrollit ovat oikeat, ne on kohdistettu oikeisiin prosesseihin ja että ne ovat kustannustehokkaita. Tietoturvan hallintaan on olemassa globaalisti tunnustettuja ja standardoituja toimintamalleja kuten ISO/IEC 27000-perhe, jonka rakenteeseen ja toimintamalleihin tutustumme myöhemmin tässä työssä.

Operatiivisella turvallisuudella tarkoitetaan organisaation tietoturvan ja siihen kohdistuvien uhkien seurantaa ja käsittelyä. Organisaatiot voivat käyttää suuria määriä resursseja asettaakseen hyökkäyksiä havaitsevia ja torjuvia järjestelmiä, mutta niistä ei ole paljoa hyötyä, mikäli niiden tuottamaa tietoa ei monitoroida ja tapahtumiin reagoida esimerkiksi tietoturvapoikkeamien hallintajärjestelmällä (Security Incident and Event Management,

[28] Karvi, Tietojenkäsittelylaitos, Helsingin Yliopisto, 2011, Tietoturvan perusteet, s. 4-5

SIEM). Tämän kaltaisten järjestelmien implementointi, operointi, ja optimointi vaativat ammattitaitoista henkilöstöä ja nämä ovat ideaali tilanteessa koottu esimerkiksi organisaation tietoturvaoperaatiokeskuksiin, jotka ovat operatiivisen tietoturvan sydämessä. Operatiivisen tietoturvan alle yleensä kuuluvat seuraavat toiminnot:

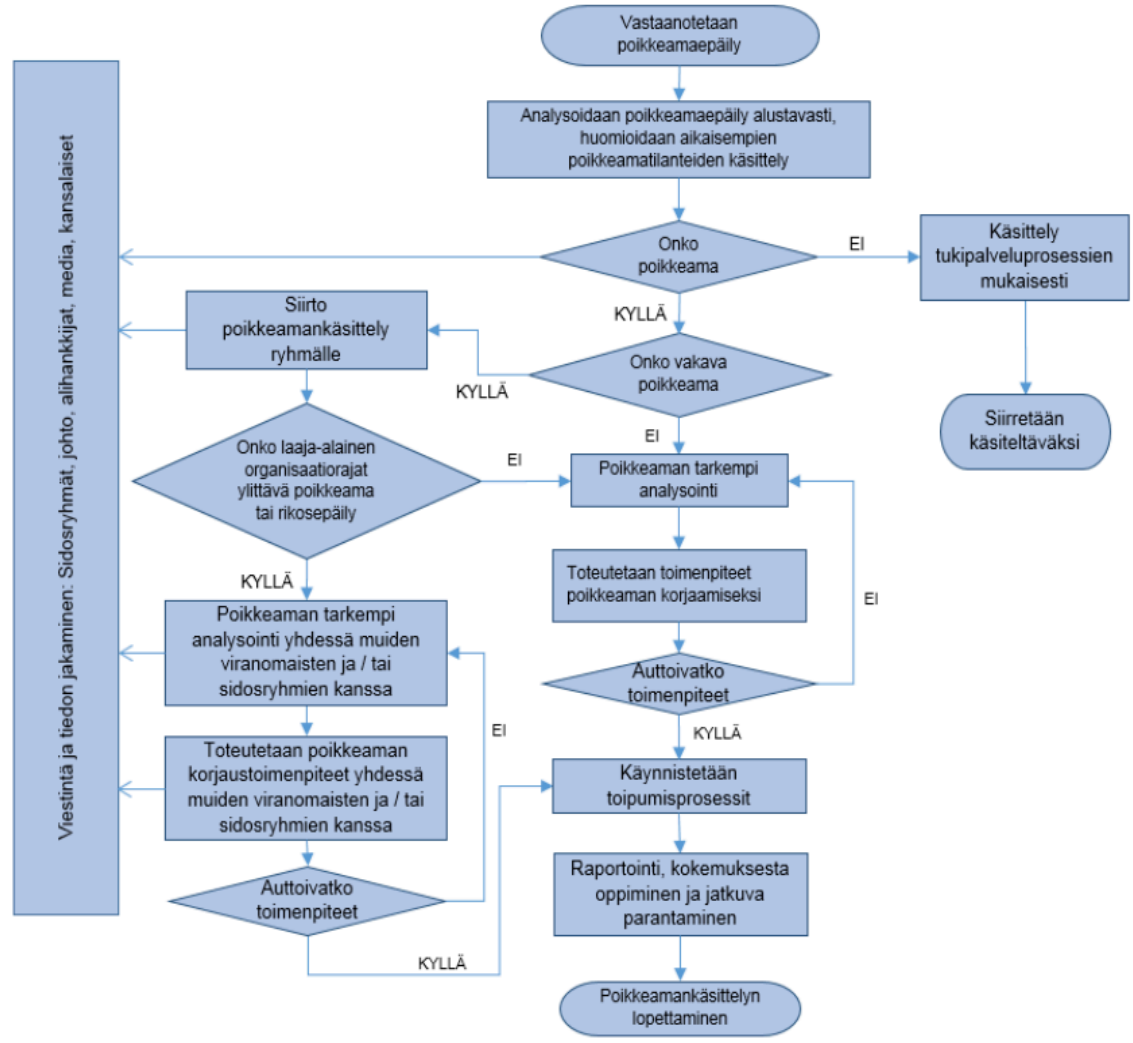


Kuva 5. Operatiivinen tietoturva

- Tietoturvaoperaatiokeskus (Security Operations Center, SOC); SOC organisoi ja operoi päivittäistä tietoturvatyötä. Sen vastuulla on tietoturvallisuuden tilannekuvan monitorointi ja reagointi mahdollisiin tietoturvapoikkeamiin. Operaatiokeskuksen henkilöstön tehtäviin kuuluu myös osallistuminen kehitystyöhön, jolla parannetaan organisaation tietoturvan tasoa.
- Tietoturvatapahtumien hallintajärjestelmä (Security Incident and Management System, SIEM); SIEM-järjestelmään kerätään turvallisuuden ja tilannekuvan kannalta tärkeät loki-tiedot eri kohteista ja kontrolleista. SIEM järjestelmä automatisoi ja korreloi eri lähteistä kerättyä tietoa ja tuottaa ajantasaista tilanne kuvaa esimerkiksi organisaation verkon tapahtumista sekä hälytykset mahdollisista haitallisista poikkeamista. Olennaisena osana SIEM järjestelmää on myös tuottaa eri standardien vaatimat seurannat ja raportit kuten esimerkiksi EU:n uusi tietosuoja-asetus edellyttää.
- Tietoturvaloukkausten hallinta ja analysointi; Tietoturvapoikkeamien hallinta koostuu useista eri osista. Perustarkoitus koko tietoturvaloukkausten ja analysoinnin hallintaprosessilla on varautua mahdollisiin poikkeamiin ja häiriötilanteisiin.

Hyvin suunnitelluilla prosesseilla ja työkaluilla pystytään minimoimaan poikkeamien ja häiriötilanteiden vaikutukset. VAHTI-ohjeen mukaan tietoturvapoikkeaman hallintaprosessi jaetaan neljään päävaiheeseen:

- Tietoturvapoikkeamien käsittelykyvyn muodostaminen
- Tietoturvapoikkeamien havaitseminen ja analysointi (tämä tapahtuu SIEM järjestelmässä)
- Tietoturvapoikkeamaan reagointi
- Tietoturvapoikkeamista toipuminen ja paluu normaaliin toimintaan.[29]



Kuva 6. Tietoturvapoikkeaman hallintaprosessi[30]

[29] VAHTI-Tietoturvapoikkeamatilanteiden hallinta, 2017. s.13.
[30] VAHTI-Tietoturvapoikkeamatilanteiden hallinta, 2017. s.15.

- Haavoittuvuuksien hallinta; Haavoittuvuuksien hallinta on toimintaa, jossa kartoitetaan organisaation käytössä olevien järjestelmien ja ohjelmiston tasoja, versioita ja niiden mahdollisia haavoittuvuuksia sekä tietenkin näiden haavoittuvuuksien paikkaamista. Organisaatioiden verkot ja järjestelmät päivittyvät jatkuvasti ja niihin tuodaan uusia tietoja ja sovelluksia, jotka mahdollisesti kytkeytyvät ulkoisiin verkkoihin. Nämä tekijät yhdessä haavoittuvuuksien kanssa muodostavat uusia mahdollisuuksia hyökkääjille päästä käsiksi organisaation tietoihin ja järjestelmiin. Siksi on äärimmäisen tärkeää, että organisaatiolla on toimiva ja testattu prosessi haavoittuvuuksien hallintaan. Paras tapa ehkäistä organisaatiota vastaan kohdistuvia uhkia on kartoittaa, ennakoida ja ennaltaehkäistä niitä jatkuvan organisoidun toiminnan kautta.
- Tiedustelu (Threat Intelligence, TI); Uhkatiedustelu on tärkeä osa riskienhallintaa ja varautumista. Organisaation tulee tietää mitä uhkia heidän toimialallaan on ja miten ne voivat mahdollisesti vaikuttaa heihin. Jos et tiedä kuka, missä, milloin ja miten voi sinun organisaatiotasi vastaan hyökätä, miten voit niitä vastaan suojautua ja varautua.

4.3 Henkilötietojen turvallisuus, EU:n tietosuoja-asetus

Tietosuoja on yksi osa tietoturvaa ja ilman hyvää tietoturvaa ei ole yhdelläkään organisaatiolla riittäviä edellytyksiä suojata hallussaan olevaa tietoa. EU:n uudessa tietosuoja-asetuksessa henkilötietojen tekniseen ja organisatoriseen turvallisuuteen keskittyvät artiklat 32-34.

4.3.1 Artikla 32

EU:n uuden tietosuoja-asetuksen 32 artikla määrittelee: *”Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet”.*[31] Koko tietosuoja-asetuksessa on oikeastaan vain kolme artiklaa, jotka ottavat jokseenkin suoraan kantaa tietosuojan edellyttämään

[31] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Artikla 32

tietoturvaan. Kuten jo aikaisemmin työssä on todettu, niin tietosuoja edellyttää tietyt teknologiset ja organisatoriset tietoturvaratkaisut, jotta tietosuoja voi toteutua.

Tietosuoja-asetuksessa monesti määritellään rekisterinpitäjä vastuulliseksi ja myös artiklat 32-34 velvoittavat rekisterinpitäjää toteuttamaan asianmukaiset tekniset ratkaisut, jotta henkilötietojen käsittely on turvattua. Artikla 32 pitää sisällään tiedon suojaamisen sen koko elinkaaren aikana aina luomisesta tuhoamiseen, mutta myös olemassaolon aikana sen siirtojen, tallennuksen, luvattoman käsittelyn, muuttamisen tai luovuttamisen osalta. Tietosuoja-asetuksen artiklat eivät kuitenkaan ota kantaa kovin syvällisesti mitä nämä tekniset tai organisatoriset keinot ovat. Artikla määrittelee vaadituiksi keinoiksi ainoastaan:

a) *henkilötietojen pseudonymisointi ja salaus;*
b) *kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;*
c) *kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;*
d) *menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.* [32]

Tämä neljän kohdan lista käsittelee aihetta todella korkealta tasolta ja jokaisen kohdan alle tulevat tekniset toimenpiteet ovat monimutkaisia ja merkittävän suuria kokonaisuuksia, joiden hallinta vaatii osaamista ja resursseja. Tämä korkean tason määrittely tekee myös mielestäni tästä erittäin vaikean toteuttaa. Kuka ja mikä määrittelee riittävän teknisen ja organisatorisen laajuuden? Tietysti, kun lähdetään määrittelemään tarvittavia toimenpiteitä ja niiden laajuutta, niiden riittävyyteen vaikuttaa kohde organisaation koko, toimiala, ydintoiminta ja miten se tulee suhteuttaa suojattavaan tietoon ja toimintaan, jotta saavutetaan riittävä tietoturvan taso. Tietoturvallisuuden hallintaan ja tekniseen arkkitehtuuriin voidaan hyödyntää saatavilla olevia globaalisti tunnustettuja standardeja kuten ISO/IEC 27000-perhe ja esimerkiksi kotimaisesti valtionhallinnossa käytetty tietoturvan toteutumista ohjaava asetus 681/2010.[33] Näihin standardeihin ja niiden tietoturvan hallinta malleihin pureudutaan syvällisemmin tämän työn luvussa 4.4.

---

[32] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Artikla 32
[33] VAHTI raportti 1/2016, EU-tietosuojan kokonaisuudistus, s. 24-25

Tutkittaessa syvällisemmin artiklan 32 vaatimuksia voidaan listata seuraavia perusvaatimuksia:

a) Henkilötietojen pseudonymisointi ja salaus:
   ”Pseudonymisoimisella’ tarkoitetaan, että kerättyjä tietoja ei voida yhdistää kohdehenkilöön ilman tarvittavia lisätietoja Yksinkertaisimmillaan tämä tarkoittaa, että kohdehenkilön tiedot korvataan esimerkiksi numerotunnisteilla, jotka taas voidaan muuttaa luettavaan muotoon yhdistämällä tunnisteet edellä mainituihin lisätietoihin. Jotta tietoturva toteutuu, tulee tällaiset pseudonymisoinnin purkavat lisätiedot säilyttää erillään ja niihin luvattoman pääsyn estämiseksi sovelletaan teknisiä ja organisatorisia toimenpiteitä, kuten salaus ja käyttövaltuushallinta.

   Henkilötiedot tulee myös salata käyttäen riittävää vahvoja nykyaikaisia salausmekanismeja/algoritmeja sekä salausavaimia. Tiedot tulevat olla salattuna kaikissa sen elinkaarenvaiheissa oli tieto sitten varastoinnissa tai liikkeessä. Kuitenkin ehkä merkittävimpiä keinoja estää tietojen päätyminen väärille henkilöille on käyttövaltuushallinta. Käyttövaltuushallinta kattaa tietojärjestelmien käyttöoikeusperiaatteiden määrittelyn ja siinä otetaan myös huomioon käyttäjä/käyttäjäryhmä kohtaiset rajoitukset. Nämä rajoitteet voivat perustua esimerkiksi käyttäjän rooliin, tiedon omistajan määrittelemiin oikeuksiin tai organisaation politiikkaan. Käyttöoikeushallintaan yhdistetään englannin kielinen termi Identity and Access Management (IAM).

b) Kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus:
   Tämä kohta on hyvin laaja alue ja kattaa lähes kaikki tietoturvan kahdeksan eri osa-aluetta ja sinänsä myös mielestäni on osittain päällekkäinen muiden lueteltujen perusvaatimusten kanssa. Luottamuksellisuus (confidentiality), eheys (integrity) ja käytettävyys (availability) ovat tietoturvan kolme kulmakiveä. Vikasietoisuutta käsitellään enemmän seuraavassa vaatimuksessa. Jotta voidaan saavuttaa tietojärjestelmien ja palveluiden luottamuksellisuus, eheys ja käytettävyys, tulee tietoturva ottaa huomioon jo erittäin aikaisessa vaiheessa järjestelmien tai toiminnan suunnittelua. Yleisesti tietoturva-alalla todetaan, että ensimmäiseksi pitää tietää mitä suojataan, mitkä ovat organisaation niin kutsutut ”kruunun jalokivet”, joiden perustalle toiminta on rakennettu ja joita pitää suojella toiminnan jatkamiseksi. Kaikki tieto ei ole samanarvoista ja ei ole kustannustehokasta ja ehkä

jopa mahdollista suojata kaikkea käytössä olevaa tietoa yhtä tarkasti. Tietoturvan tulee olla myös ylhäältä johdettua, eli organisaation johdon pitää sitoutua myös toteuttamaan organisaation tietoturva strategiaa ja politiikkaa.

Kansallinen VAHTI-ohje listaa vaatimuksia hyvälle tietoturvalle seuraavasti:

1. *”Riskianalyysi tietoturvan mitoittamisen apuvälineenä. Asetus velvoittaa rekisterinpitäjää ottamaan huomioon uusimman tekniikan ja toteuttamiskustannukset sekä toisaalta arvioimaan tietoturvakeinojen kohtuullisuutta verrattuna arvioituun riskiin.”* Riskianalyysin perusteella organisaatiossa voidaan määritellä mitä tietoa pitää suojata ja millä tasolla. Riskianalyysi ja suojattavan tiedon tunnistaminen auttaa myös budjetoinnin kanssa, kun pitää määritellä mikä on mahdollista annettujen resurssien rajoissa, mutta myös priorisoinnissa, kun pitää päättää mitä suojataan ja mitä ei. Erittäin harvassa organisaatiossa tällä hetkellä tietoturva budjetit ja käytännön resurssit ovat lähelläkään riittävää tasoa ja priorisointi on pakollinen paha.

2. *”Turva-arkkitehtuuri, turvallinen verkko- ja järjestelmäarkkitehtuuri sisältäen esimerkiksi asianmukaiset palomuurit, verkkojen eriyttämisen, palvelinten kovennukset sekä henkilötietojen ja tietojen siirtoväylien salaamisen.”* Tämä perinteisesti mielletään IT-osastojen asiaksi vaikkakin siellä syvällinen tietoturva osaaminen harvoin riittää muuhun kuin itse turvallisuusjärjestelmien ylläpitoon. Teknisen tietoturvan peruspilarit, kuten anti-virus ohjelmat, palomuurit, IDS-järjestelmät ovat edelleenkin tarvittavia, mutta aika on ajamassa ohitse näistä perinteisistä niin kutsutuista ”sormenjälkiin” tai tunnisteisiin perustuvista järjestelmistä. Toki edelleenkin suurin osa haittaohjelmista tai hyökkäyksistä jää näiden perinteisten torjuntamekanismien haaviin, mutta uudet ja monesti ne vaarallisimmat hyökkäykset eivät. Uudemmat järjestelmät joiden havainnointi perustuu poikkeavan käytöksen havainnointiin ja edistyneeseen ”sandboxing” tekniikkaan joilla voidaan havaita ja torjua myös ennestään tuntemattomia haittaohjelmia.

3. *”Tietojärjestelmien hankinta, kehitys ja ylläpito. Tietoturvavaatimusten määrittäminen hankintaa ja kehitystä varten. Henkilötietojen käytön rajoittaminen tietojärjestelmien testauksessa. Tietoturvatestauksen suorittaminen järjestelmien hyväksyntätestauksen yhteydessä. Henkilötietoja käsittelevien*

järjestelmien ylläpitohenkilöstön sijainnin huomioiminen." Tietoturvallisuus tulee ottaa huomioon jo aikaisessa vaiheessa, jolloin tarvittavien suojamekanismien lisääminen on vielä helppoa ja kustannustehokasta. Uusia järjestelmiä hankittaessa on ne testattava, jotta voidaan nähdä niiden suojamekanismien riittävyys esimerkiksi standardoinnin saavuttamiseksi. Järjestelmien jatkuvasta testauksesta tulee myös huolehtia koko järjestelmän elinkaaren ajan. Esimerkiksi uudet päivitykset teknologiaan tai ohjelmistoon saattavat myös avata uusia haavoittuvuuksia, joita hyökkääjät voivat hyödyntää. Alan terminä tälle toiminnalle on haavoittuvuuksien ja päivitysten hallinta (Vulnerability and patch management). Kyseinen prosessi pitää sisällään ihannetilanteessa kaikkien käytössä olevien järjestelmien ja ohjelmistojen aikataulutetun skannaamisen ilmoitettujen haavoittuvuuksien varalta, skannausten perusteella tehtävät päivitykset, niiden seuranta ja raportointi. Kyseessä on erittäin tärkeä prosessi tietoturvan kannalta, mutta se on myös erittäin aikaa ja resursseja vievä.

4. *"Omaisuuden ja tiedon hallinta. Tietovälineiden käsittely sekä tiedon luokittelu ja luokitellun tiedon käsittelyohjeistukset. Henkilöstölle tulee olla selvää, miten henkilötietoja on sallittua käsitellä esimerkiksi pilvipalveluun tallentamisessa, sähköpostilla siirtämisessä ja siirrettäville tietovälineille tallentamisessa. Valtionhallinnossa suojaustasot (IV – III – II – I) määräävät tiedon luokittelua ja käsittelyä."* Kohdassa 1. Riskianalyysi käsittelimme jo osittain tätä aihetta. Organisaation tulee tietää mitä tietoa käsitellään ja varastoidaan, missä sitä säilytetään ja minkä arvoista tieto on organisaation toiminnalle. Kaikki tieto ei ole saman arvoista ja kuten valtionhallinnossa niin myös yksityisellä sektorilla tiedot luokitellaan niiden luottamuksellisuuden perusteella. Yksityisellä puolella perinteinen jaottelu on: julkinen, luottamuksellinen ja sisäinen. Tietoturvapolitiikka määrittelee, miten ja missä tietoa kussakin turvallisuusluokassa voidaan käsitellä, siirtää, varastoida tai tuhota. Mikäli organisaatiossa ei aikaisemmin ole ollut käytössä tietojen luokittelua, sen käyttöönotto on todella merkittävä projekti, mutta pakollinen mikäli kriittiset tiedot halutaan suojata riittävällä tasolla. Tähän projektiin tarvitaan koko organisaation resursseja ja sitä ei voi suorittaa vain tietoturva- tai IT-asiantuntija. Kriittinen tieto kun usein liittyy organisaation ydintoimintaan (liiketoimintaan) ja tällöin parhaat asiantuntijat tulevat organisaatioista, jotka tiedon omistavat.

5. *”Henkilöstöturvallisuus. Henkilöstön tietoturvatietoisuuden ja osaamisen varmistaminen koulutuksilla ja ohjeilla. Vaitiolo- ja salassapitosopimukset henkilöstön sekä alihankkijoiden kanssa. Tarvittaessa ja lain mahdollistaessa tehtävät henkilöiden turvallisuusselvitykset.”* Käytännön kokemuksesta voidaan todeta, että suurin uhka tietoturvan toteutumiselle on ihminen. Kun tietoturvasta tehdään liian vaikeaa tai sitä ei jalkauteta henkilöstölle ymmärrettävässä muodossa ja perusteltuna, on ihmisellä tapana mennä sieltä mistä aita on matalin ja löytää keinoja kiertää asetettuja ”esteitä”. Myös erilaiset organisaatio ja maakohtaiset tietoturvastandardit ja ohjeistukset aiheuttavat päänvaivaa nykyaikaisissa ulkoistus toimintamalleissa. Vaikkakin organisaation sisällä noudatetaan tiettyä politiikkaa, ei ole takeita, että esimerkiksi IT-ulkoistuskumppani tai pilvipalvelujen tarjoaja toimii samalla tasolla. Esimerkkinä organisaatio, joka käsittelee luottokorttitietoja, heidän tulee täyttää PCI-DSS-standardin vaatimukset ja tämä koskettaa myös heidän ulkoistuskumppaneitaan ja palveluntarjoajia. Myös taustaselvitykset ovat nykyaikaa, mutta Suomessa nämä ovat hyvinkin pitkälti rajoittuneet suojelupoliisin tekemään kevyeen tarkistukseen. Globaaleissa organisaatioissa nämä tarkistustoimet on osittain ulkoistettu niihin erikoistuneille turvallisuusyhtiöille. Heidän tarkistukset ulottuvat perinteisen rikosrekisterien tarkistusta pidemmälle ja tällöin tarkistetaan esimerkiksi henkilön ansioluettelon tiedot ottamalla yhteyttä kaikkiin relevantteihin tahoihin. Näiden lisäksi voidaan suorittaa kattava avoimien lähteiden (internet, sosiaalinen media) haku löytääkseen mahdollisesti haitallisia tekijöitä tai kontakteja, jotka saattavat aiheuttaa riskejä varsinkin täytettäessä roolia, joka käsittelee erittäin sensitiivistä materiaalia.

6. *”Toimittajien ja sopimusten hallinta. Tietoturva- ja tietosuojavaatimusten määrittely sopimuksen/hankinnan kohteelle ja alihankkijoille. Sovittava tietoturvan ja tietosuojan hallinnan menettelyt, mukaan lukien henkilötietojen käsittelyn seuranta ja valvonta sekä tietoturvaraportointi ja tietoturvapoikkeamien hallinta.”* Kohdassa viisi sivuttiin jo aihetta liittyen ulkoistuskumppaneiden ja palveluntarjoajien tietoturvastandardeihin. Nykyiset teknologiset ratkaisut kuten IoT, pilvipalvelut ja perus IT-ulkoistukset mahdollistavat merkittäviä parannuksia organisaation toiminnan tehokkuuteen ja taloudellisuuteen, mutta ne samalla avaavat uusia suuria rajapintoja riskeille. Ei enää riitä,

että oman organisaation toimintamallit täyttävät lain ja standardien edellytykset, vaan pitää myös varmistaa, että myös eri kolmansien osapuolien toiminta on samalla tai vähintäänkin riittävällä tasolla. Näitä edellytyksiä voidaan hallinnoida ainoastaan velvoittamalla kolmannet osapuolet toteuttamaan riittävää tietoturvaa sopimuksien kautta. Toki pelkkä sopimus ei takaa mitään, vaan sopimusten ja vaatimusten täyttymistä tulee seurata ja auditoida koko sopimuksen ajan, sekä edellyttää tarvittavaa raportointia näiden vaatimusten toteutumisesta.

7. *”Käsittelyn valvonta ja seuranta. Rekisterinpitäjän tulee voida jälkikäteen todentaa lokitiedostoista, kuka on suorittanut henkilötietojen haun järjestelmästä, mitä henkilötietoja on katsottu, muutettu, lisätty tai poistettu sekä milloin toimenpide on suoritettu (aikaleima). Menettelyt, joilla lokitiedostoja seurataan ja miten epäillyt väärinkäytökset käsitellään, tulee suunnitella etukäteen. Tärkeää on myös varmistaa, että tietojen käsittelyn seuranta- ja valvontatehtävät ovat selkeästi vastuutettu ja riittävästi resursoidut. Myös mahdolliset seuraamukset henkilötietojen väärinkäytöksistä olisi hyvä kartoittaa ja määritellä etukäteen. Rekisteröityjen viestinnän osana olisi syytä viestiä myös tietojen käsittelyn seurannasta ja mahdollisten väärinkäytösten seuraamuksista. Seurantaa on mahdollisuuksien mukaan hyvä suorittaa automatisoidusti, sillä lokia muodostuu tyypillisesti hyvin paljon.”* Perusteita lokien hallinnalle on yleensä kolme; liiketoiminnan jatkuvuus, toiminnan tehostaminen sekä parempi riskienhallinta. Oli päämotiivina sitten mikä tahansa tulee lokien keräämisen perustua organisaation politiikkaan, joka määrittää tarpeen ja käytettävän prosessin. Jotta lokien kerääminen on laadukasta, sen tulee olla suunnitelmallista aina keräämisestä poistamiseen. Käytännössä testatut parhaat toimintamallit suosittelevat keräämään lokitiedot keskitetylle palvelimelle, jossa tieto säilytetään ja käsitellään. Keskitetystä sijainnista on tietoa myös helpompi jalostaa haluttuihin eri käyttötarkoituksiin, oli sitten kyseessä käytönseuranta, kuten VAHTI-ohjeessa käsitellään tai sitten perinteisten tieturvatapahtumien analysointi. Puhuttaessa tiedostojenkäsittelyn valvonnasta ja seurannasta usein käytetään englanninkielistä termiä File Integrity Monitoring (FIM). Tätä toimintaa varten on olemassa useita eri palveluntarjoajia, jotka tarjoavat omia ohjelmistojaan. Pelkästään tiedon katsomisen, muuttamisen tai poistamisen valvonta ei riitä, vaan organisaation pitäisi myös

pystyä monitoroimaan tiedon siirtämistä verkossa ja varsinkin jos tietoa ollaan siirtämässä turvallisen verkon ulkopuolelle. Tätä toimintaa varten on olemassa Data Loss Preventation (DLP) ohjelmistoja, jotka pystyvät tunnistamaan siirrettävää tietoa esimerkiksi tietosuojaluokituksen, avainsanojen ja tiedoston metadatan perusteella. Tällöin pystytään havainnoimaan esimerkiksi vahingossa tai tahallaan väärin lähetetty tiedosto, pysäyttämään se tai vähintäänkin jäljittämään lähettäjä ja vastaanottaja.

8. *”Tietoturvallisuuden hallinta. Tietoturva-organisaation määrittäminen, roolit ja vastuut sisältäen henkilöstölle määriteltävät tietoturvavastuut. Tietoturvan hallintatehtävien määrittäminen vuosikelloon. Tietoturvan säännöllinen mittaaminen, todentaminen ja kehittäminen. Tietoturvaa voidaan todentaa esimerkiksi teknisellä testauksella ja hallinnollisten prosessien auditoimisella.”* Tietoturvallisuus on nostanut profiiliaan merkittävästi viimeisten vuosien aikana ja tämä trendi tulee vain korostumaan tulevaisuudessa uusien lakien ja standardien vaatimusten myötä. Tänä päivänä varsin harvassa organisaatiossa on varsinaista tietoturvaorganisaatiota, jolla olisi kokonaisuudessaan vastuu ja resurssit tietoturvan toteuttamisesta. Erittäin usein kyseessä on yksittäinen henkilö IT-organisaation sisällä, jolla ei ole budjettia tai riittävää vaikutusmahdollisuutta. Monessa suomalaisessa suuressa organisaatiossa tietoturvapäällikkö/johtaja raportoi IT-organisaation johdolle eikä hänellä ole pääsyä esimerkiksi johtoryhmän eteen, näin ollen häneltä usein puuttuu mahdollisuudet vaikuttaa. Tietoturvaa tulee kuitenkin johtaa ”ylhäältä käsin”. Johto hyväksyy organisaation tietoturvastrategian ja he ovat myös loppukädessä vastuussa sen toteutumisesta sekä mahdollisista seuraamuksista, mikäli suojaus pettää. Kun strategia ja prosessit on suunniteltu ja jalkautettu niitä ei tule unohtaa, vaan niitä tulee testata riittävän usein, jotta toiminta poikkeustilanteessa olisi suunnitelman mukaista ja nopeaa. Testaaminen voi tarkoittaa esimerkiksi olemassa olevien suunnitelmien auditointia ja niiden vertaamista nykyhetken ja lähitulevaisuuden riskeihin. Testaaminen pitää myös ulottaa aina käytännön toimintaan asti, miten tietoturvatiimi toimii poikkeaman sattuessa, milloin organisaation johto tarvitaan mukaan päätöksen tekoon ja milloin ja miten asiasta pitää/joudutaan tiedottamaan organisaation ulkopuolelle. Mitä nopeammin poikkeama saadaan hallintaan, sitä suuremmat ovat mahdollisuudet minimoida seuraamukset sekä mahdollistaa nopea toipuminen. Kirjoitettu

strategiat ja suunnitelmat vanhenevat todella nopeasti nykyaikaisen teknologian ja siitä riippuvaisen liiketoiminnan kehityksen vauhdissa, joten testauksen kautta saadut opit voidaan päivittää suunnitelmiin. [34]

c) Kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa:

Toiminnan jatkuvuuden suunnitelma (Business Continuation Plan, BCP) ja toipumissuunnitelma (Disaster Recovery Plan, DRP) pitäisi olla jokaisen organisaation arkipäivää. Sinänsä tämä ei ole mitään uutta, vaan kyseessä on IT toimintamalli, jolla huolehditaan esimerkiksi varmuuskopioinnista, järjestelmien kapasiteetista, varajärjestelmistä ja varayhteyksistä mahdollisiin epäsuotuisiin tilainteisiin. Aikaisemmin nämä suunnitelmat ehkä enemmän keskittyivät fyysisiin tilanteisiin kuten tulipaloihin, tulviin, sähkökatkoihin ja niin edelleen, mutta nykyinen verkottunut yhteiskunta ja sitä seuraava verkkorikollisuus on nostanut uusia ja erilaisia uhkia joihin pitää varautua. Esimerkkeinä mainittakoon palvelunestohyökkäykset tai kaikille jo niin tutut ”ransomware” kiristysohjelmat. Kyseessä on siis tietojen saatavuus kaikissa tilanteissa, sekä palautuminen ongelmatilanteesta mahdollisimman nopeasti. Perinteisinä ratkaisuina ovat esimerkiksi järjestelmien ja yhteyksien kahdentaminen joko samassa toimipisteessä tai sitten hajauttamalla useampaan toimipisteeseen sekä tietojen jatkuva varmuuskopiointi. Jälleen kerran on todettava, että kun edellä mainitut suunnitelmat ovat olemassa, niitä pitää auditoida, testata ja päivittää järjestelmällisesti, jotta jokainen tietää mitä pitää tehdä poikkeaman sattuessa ja järjestelmät/palvelut saadaan taikaisin käytettäviksi minimaalisella katkoksella ja vahingolla.[35]

d) Menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi:

Tämä on olennainen osa tietoturvaa ja riskienhallintaa. Toimintaympäristö, teknologiat ja uhat muuttuvat jatkuvasti ja organisaation tekemiä prosesseja ja teknisiä ratkaisuja tulee auditoida ja kehittää jatkuvasti. Toimintaan kohdistuvia riskejä

[34] VAHTI raportti 1/2016, EU-tietosuojan kokonaisuudistus, s.24-26.
[35] Thomas Tom, 2004, Verkkojen Tietoturva, s. 366-367.

ja uhkia tulee analysoida vaativatko ne uudenlaisia torjuntakeinoja. Olemassa olevia järjestelmiä ja ohjelmistoja tulee päivittää uusien haavoittuvuuksien varalta sekä huolehtia tehtyjen muutosten jäljitettävyydestä[36].

4.3.2 Artikla 33

Artikla 33 määrittelee velvollisuuden ilmoittaa tapahtuneesta tietoturvaloukkauksesta valvovalle viranomaiselle. Mikäli organisaatioissa tapahtuisi tietoturvaloukkaus, joka kohdistuu esimerkiksi henkilötietoihin olisi organisaation ilmoitettava siitä mahdollisuuksien mukaan ja ilman aiheetonta viivästystä 72 tunnin kuluessa toimivaltaiselle valvontaviranomaiselle. Poikkeuksena tähän voidaan pitää tilannetta, jossa tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä, joka kohdistuu luonnollisten henkilöiden vapauksiin tai oikeuksiin. Mikäli ilmoitus jätetään tekemättä tai se viivästyy, tulee toimittaa perusteltu selvitys valvontaviranomaiselle.

Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta valvontaviranomaisille tehtävän ilmoituksen tulee pitää sisällään vähintään seuraavat tiedot:

a) *Kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;*
b) *Ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;*
c) *Kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;*
d) *Kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturva loukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.*[37]

Edellä mainitun ilmoituksen lisäksi artikla 33 velvoittaa, että organisaation rekisterinpitäjän tulee dokumentoida kaikki henkilötietoihin kohdistuvat tietoturvaloukkaukset. Tämän dokumentoinnin perusteella valvontaviranomaisen on voitava tarkistaa, että artiklaa on noudatettu. Tämä edellyttää, että organisaation dokumentointi on riittävän tarkkaa ja pitää sisällään kaikki oleelliset tietoturvaloukkaukseen liittyvät tiedot, kuten loukkauksen vaikutukset ja toteutetut korjaavat toimenpiteet.

---

[36] Thomas Tom, 2004, Verkkojen Tietoturva, s. 366-367.
[37] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Artikla 33

Artiklan 33 vaatimusten toteuttamiseen liittyy olennaisena osana tekninen ja operatiivinen tietoturvallisuus. Mikäli organisaatiolla ei ole tarvittavaa havainnointikykyä erilaisten teknisten tietoturvajärjestelmien kautta ja toimivaa tietoturvatapahtumien hallintajärjestelmää (SIEM) ja sen tuottamaa tilannekuvaa, miten organisaatiossa voidaan ylipäätänsä havaita tietomurto, dokumentoida se riittävällä tasolla saati sitten raportoida siitä viranomaisille.

4.3.3 Artikla 34

Artikla 34 edellyttää henkilötietoihin kohdistuneesta tietoturvaloukkauksen ilmoittamisesta rekisteröidylle jonka tietoihin kyseinen loukkaus on kohdistunut. EU:n uuden tietosuoja-asetuksen yhtenä perusajatuksena on antaa rekisteröidyille enemmän oikeuksia hallita tietojaan ja sitä, miten ja missä niitä käytetään. Näin ollen voidaan pitääkin vähimmäisvaatimuksena, että rekisteröidyn tietoihin kohdistuneesta loukkauksesta ilmoitetaan valvontaviranomaisen lisäksi myös suoraan rekisteröidylle. Tätä ilmoitusta edellytetään, kun on todennäköistä, että tietoturvaloukkaus aiheuttaa suuren riskin luonnollisten henkilöiden vapauksille ja oikeuksille. Kuten artiklassa 33 myös artikla 34 edellyttää rekisterinpitäjää tekemään ilmoituksen ilman aiheetonta viivästystä. Rekisteröidylle tehtävässä ilmoituksessa on kuvattava yksinkertaisella ja selkeällä kielellä loukkauksen kohde, luonne ja annettava vähintäänkin artiklan 33, 3 kohdan b, c ja d alakohtien tiedot.

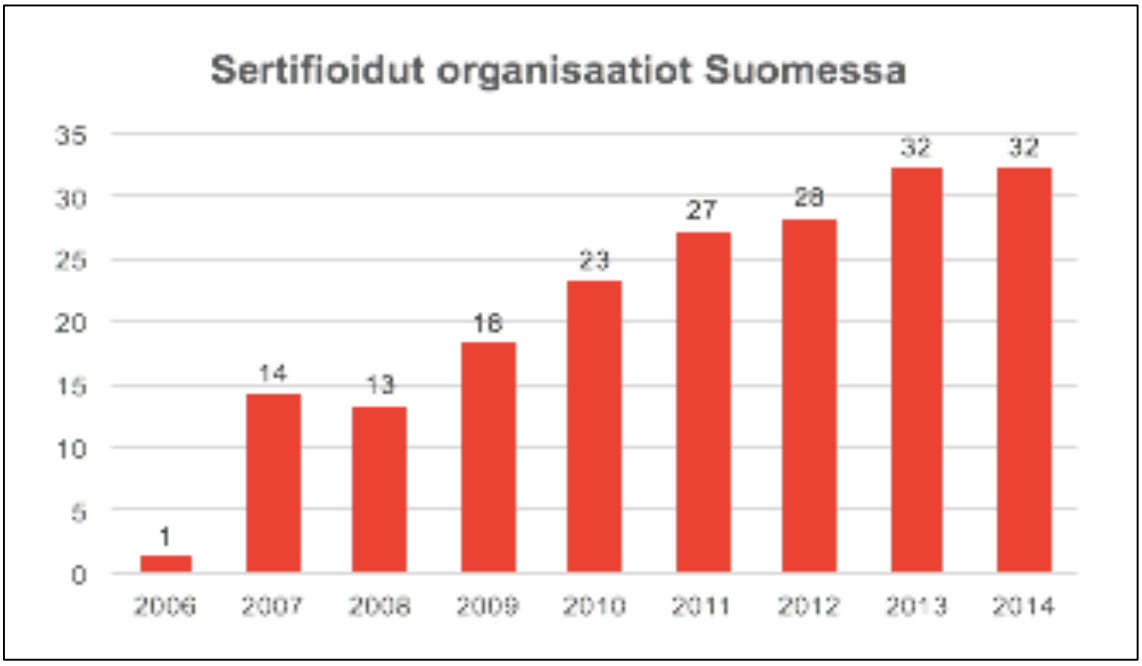
Rekisteröidylle tehtävää ilmoitusta ei vaadita, mikäli jokin seuraavista edellytyksistä täyttyy:

a) *rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta;*
b) *rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu;*

c) *se vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.* [38]

4.4 Tietoturvallisuuden yleisesti tunnustettuja standardeja

Tietosuojaan ja tietoturvaan kohdistuvat uudet lainsäädännöt tulevat kasvattamaan organisaatioiden tarvetta sertifioitua erilaisia kansainvälisiä standardeja vastaan kuten ISO/IEC 27001. Esimerkiksi 2018 voimaan tuleva EU:n verkko- ja tietoturvallisuusdirektiivi (EU) 2016/1148, joka on jäänyt julkisessa keskustelussa jokseenkin tietosuoja-asetuksen varjoon, suorastaan kannustaa organisaatioita direktiivin artiklassa 19 käyttämään verkko- ja tietojärjestelmien turvallisuuden kannalta merkityksellisiä eurooppalaisia tai kansainvälisesti hyväksyttyjä standardeja.[39] Tälle hetkellä esimerkiksi suomessa ISO/IEC 27001 standardin käyttöönotot ovat yleistyneet, mutta Suomen Standardoimisliiton SFS ry:n julkaisemien lukujen mukaan, näiden organisaatioiden lukumäärä ei edes Suomen mittakaavassa ole kovinkaan merkittävä;



Kuva 7. ISO/IEC 27001 sertifioidut organisaatiot suomessa.[40]

[38] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Artikla 34
[39] Euroopan neuvoston ja parlamentin direktiivi (EU) 2016/1148. Artikla 19
[40] Suomen Standardisoimisliitto SFS ry, Kalvosarja oppilaitoksille. 2015. s.10

4.4.1 ISO/IEC 27000-perhe

ISO/IEC 27000 on kansainvälisten ISO- ja IEC organisaatioiden luoma ja ylläpitämä standardiperhe, jonka yhteinen otsikko on "Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät".[41] Hallintajärjestelmien kansainväliset standardit tarjoavat malleja, joita organisaatiot voivat seurata ottaessaan käyttöön omia tietoturvallisuuden hallintajärjestelmiä (ISMS). ISO/IEC mallit ovat koonneet kansainväliset tietoturva-alan huippuasiantuntijoista koostuva asiantuntijakomitea.

ISMS-standardien perhe on tarkoitettu auttamaan organisaatioita ottamaan käyttöön sekä käyttämään tietoturvanhallintajärjestelmiä omassa toiminnassaan. ISO/IEC 27000 standardit eivät ota kantaa siihen mitä toimialaa tai kokoluokkaa kohde organisaatio edustaa vaan se on sovellettavissa kaiken tyyppisissä ja kokoisissa organisaatioissa. ISO/IEC 27000-perhe koostuu seuraavista kansainvälisistä standardeista:

- ISO/IEC 27000, *Information security management systems — Overview and vocabulary,*
- ISO/IEC 27001, *Information security management systems — Requirements,*
- ISO/IEC 27002, *Code of practice for information security controls,*
- ISO/IEC 27003, *Information security management system implementation guidance,*
- ISO/IEC 27004, *Information security management — Measurement,*
- ISO/IEC 27005, *Information security risk management,*
- ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems,*
- ISO/IEC 27007, *Guidelines for information security management systems auditing,*
- ISO/IEC TR 27008, *Guidelines for auditors on information security controls,*
- ISO/IEC 27009, *Sector-specific application* of *ISO/IEC 27001 — Requirements,*
- ISO/IEC 27010, *Information securit y management for inter-sector and inter-organizational,*

[41] Suomen Standardisoimisliitto SFS ry, Kalvosarja oppilaitoksille. 2015. s.10

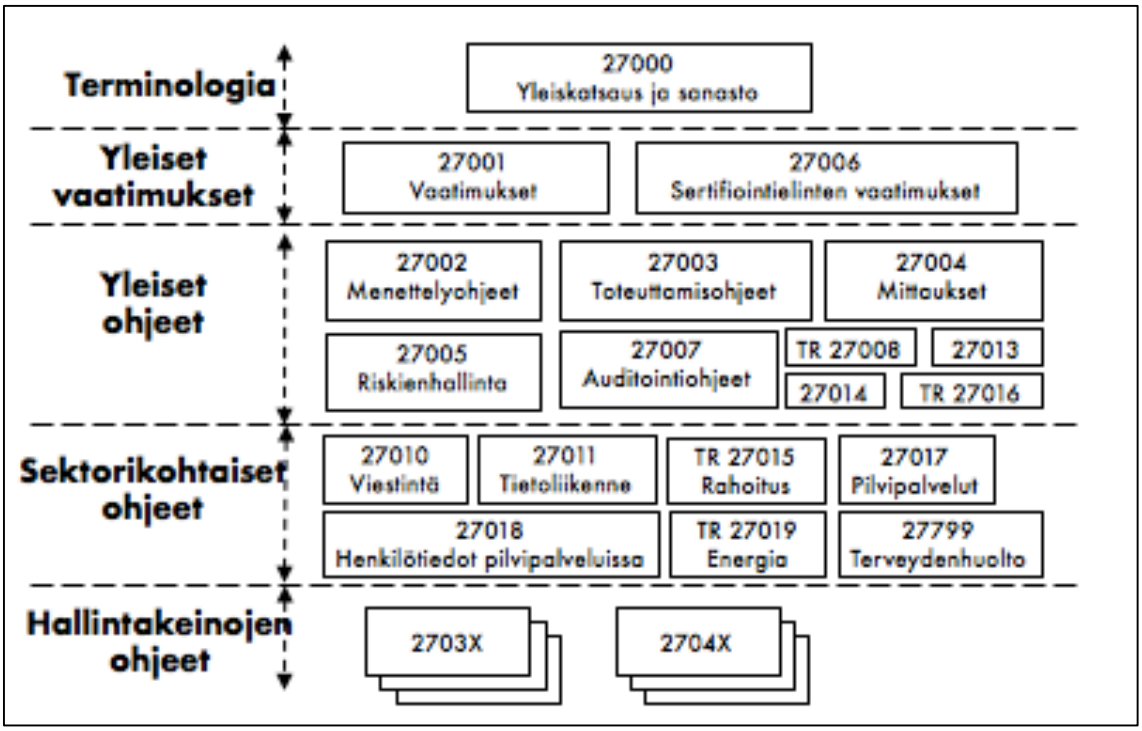
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations communications based on* ISO/IEC 27002,
- ISO/IEC 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1,*
- ISO/IEC 27014, *Governance of information security,*
- ISO/IEC TR 27015, *Information security management guidelines for financial services,*
- ISO/IEC TR 27016, *Information security management — Organizational economics,*
- ISO/IEC 27017, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services,*
- ISO/IEC 27018, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,*
- ISO/IEC 27019, *Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.*[42]

Yllä listattujen standardien lisäksi on vielä olemassa hallintakeinojen ohjeet (2703X ja 2704X –sarjat).

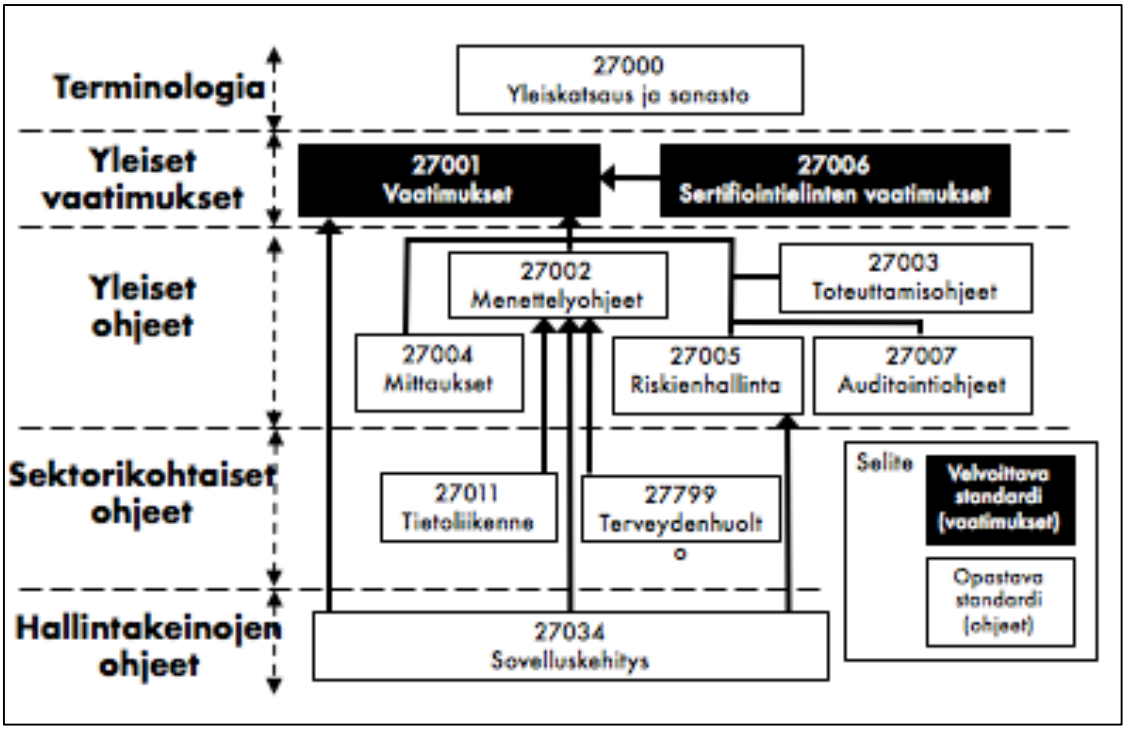
ISO/IEC 27000-standardit on luokiteltu viiteen eri kategoriaan;

1. Terminologia
2. Yleiset vaatimukset
3. Yleiset ohjeet
4. Sektorikohtaiset ohjeet
5. Hallintakeinojen ohjeet

[42] ISO/IEC 27000:2016(E). s.7-8.



Kuva 8. ISO/IEC 27000-luokittelu.[43]



Kuva 9. ISO/IEC 27000 standardien väliset suhteet.[44]

[43] Suomen Standardisoimisliitto SFS ry, Kalvosarja oppilaitoksille. 2015. s.21.
[44] Suomen Standardisoimisliitto SFS ry, Kalvosarja oppilaitoksille. 2015. s.22.

ISO/IEC 27000 standardiperheestä ainoastaan standardiin ISO/IEC 27001 voi organisaatio virallisesti sertifioitua. ISO/IEC 27001 määrittelee ne vaatimukset, jotka koskevat dokumentoidun tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, käyttämistä, valvontaa, katselmointia, ylläpitoa ja parantamista ottaen huomioon organisaation yleiset liiketoimintariskit. Standardi myös määrittelee vaatimukset turvamekanismien toteuttamista varten yksittäisen organisaation tai sen osien yksilöllisten tarpeiden mukaisesti. Tietoturvallisuuden hallintajärjestelmä luodaan takaamaan riittävien ja asianmukaisesti mitoitettujen turvamekanismien valinta.[45]

4.4.2 Katakri

Kansallinen turvallisuusauditointikriteeristö eli Katakri, on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä ja mahdollisuutta suojata viranomaisen salassa pidettäväksi määrittelemää tietoa. Poiketen ISO/IEC 27000-perheen standardeista Katakri itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia vaan sen vaatimukset ovat kokoelma kansallisen lainsäädännön ja Suomea sitovien kansainvälisten tietoturvallisuusvelvoitteiden määrittelemiä. Katakrin keskeisimmät vaatimuslähteitä ovat voimassa olevat lainsäädännöt, kuten valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), sekä EU:n neuvoston turvallisuus säännöt (2013/488/EU).[46]

Ensimmäinen Katakri julkaistiin vuonna 2009 ja tämän jälkeen siitä on julkaistu kaksi päivitettyä versiota, Katakri II (2011) ja viimeisin versio Katakri III, joka julkaistiin 2015. Katakrin kolmatta versiota ei voida oikeastaan pitää enää ainoastaan päivitettynä versiona, vaan siinä on nähtävissä merkittäviä muutoksia ja niistä ehkä suurimpana on riskilähtöinen lähestymistapa. Uuden lähestymistavan mukaan, turvallisuuden vaatimuksia lähdetään arvioimaan riskiarvion perusteella ja arviosta tehdyn tulkinnan perusteella määritellään ja suhteutetaan tarvittavat suojausmenetelmät. Arvioitaessa suojattavaan kohteeseen kohdistuvaa riskiä, tulee ottaa huomioon muun muassa kohteen luokitus, tiedon käsittely-ympäristö sekä tiedossa olevat mahdolliset uhat. Poiketen aikaisemmasta on myös riskiarvion tekemisestä suojattavalle kohteelle tullut pakollinen vaatimus kaikilla suojaustasoilla. Katakrin uudessa versiossa on myös huomattavaa sen vaatimusten muuttuminen lyhyiksi ja ytimekkäiksi ja ne muistuttavat huomattavasti enemmän ISO/IEC

[45] Suomen Standardisoimisliitto SFS ry, Kalvosarja oppilaitoksille. 2015. s.29.
[46] Katakri 2015, s.3

27001 standardin vaatimuksia ja muutoinkin se pitää sisällään enemmän viittauksia aikaisemmin esiteltyyn ISO/IEC 27000-standardiperheeseen.

Katakrin vaatimukset on jaoteltu kolmeen eri osa-alueeseen;

1. *Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys. Turvallisuusjohtami- sen osa-alueessa on kuvattu perustaso, jonka vaatimukset kohdeorganisaation tulee täyttää.*
2. *Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Organisaa- tion tilat voidaan salassa pidettävien tietojen käsittely- ja säilyttämistarpeen perus- teella jakaa kolmeen alueeseen: hallinnollinen alue, turva-alue ja tekninen turva-alue.*
3. *Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekni- selle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset. Tämä osa-alue jakautuu kolmeen käsiteltävän tiedon mukaiseen suojaustasoon (ST IV, ST III, ST II).*[47]

Katakrin vaatimukset on esitetty siten, että niiden toteuttaminen on mahdollista käyttäen erilaisia toteutustapoja. Eri vaatimusten yhteydessä on myös esitelty erilaisia tapoja, miten vaatimukset voidaan täyttää. Katakrin esittämät toteutusvaihtoehdot eivät ole kuitenkaan sitovia, vaan ne ovat suosituksia, jotka on koottu toimialan parhaista käytännöistä. Näitä samoja käytäntöjä löytyy myös myöhemmin esiteltävästä VAHTI-ohjeistuksesta, sekä EU:n turvallisuussääntöjen suuntaviivoista ja ohjekirjoista.

4.4.3 VAHTI

Valtionvarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Tämän ohjaamista vasten on koottu VAHTI-organisaatio, joka on valtionvarainministeriön alaisuudessa toimiva johtoryhmä / koordinaatioelin, jonka vastuulla on kehittää ja ohjata julkisen hallinnon digitaalista turvallisuutta, sekä ohjata niitä toteuttavien organisaatioiden valmistelua ja yhteistyötä. ”*VAHTIn asema on kirjattu voimassa oleviin val-*

[47] Katakri 2015, s.3-4

tioneuvoston periaatepäätöksiin Suomen kyberturvallisuusstrategiasta 2013 ja valtionhallinnon tietoturvallisuuden kehittämisestä 2009. Lisäksi VAHTIlla on keskeinen rooli kyberturvallisuusstrategian toimeenpano-ohjelman toteuttamisessa." [48]

Valtionhallinnossa on tunnistettu turvallisuuteen kohdistuvat haasteet, joita julkishallinnon palveluiden digitalisaatio tuo mukanaan ja siksi VAHTIn toimintaa ja tuloksellisuutta on kehitetty ja resursseja vahvistettu. VAHTI-organisaation yksi merkittävimmistä tehtävistä onkin kehittää ja määritellä valtionhallinnon digitaalisten palveluiden turvallisuusvaatimuksia. Tähän toimintaan kuuluvat ohjeistuksen lisäksi myös erilaiset turvallisuuteen ja jatkuvuuteen liittyvät tarkistukset, arvioinnit sekä hyväksynnät, mutta myös kyberturvallisuusharjoitustoiminnan edistäminen eri valtionhallinnon, sekä valtion kannalta kriittistä infrastruktuuria ylläpitävien yksityisten organisaatioiden kanssa.

VAHTI-johtoryhmän alaisuudessa, toimivat VAHTI-sihteeristö, asiantuntijajaosto sekä eri toimialueiden asiantuntijaryhmiä. Näiden organisaatioiden tehtävänä on vastata valtionhallinnon VAHTI-toimintaan liittyvien linjausten, ohjeiden, henkilöstön koulutuksen ja materiaalin tuottamisesta. Tämän lisäksi vastuulle kuuluu toimintamallien kehittäminen, joilla vastataan valtionhallintoon tai kriittiseen infrastruktuuriin kohdistuviin laaja-alaisiin tietoturva- ja/tai kyberturvallisuuspoikkeamiin tai häiriötilanteisiin.

VAHTI-asiantuntijaryhmät on jaoteltu viiteen eri toimialueeseen:

1. *Johtaminen ja riskienhallinta.*
2. *Toiminnan jatkuvuuden hallinta*
3. *Turvallisuus kehittämisessä.*
4. *Turvallisuuden ylläpito*
5. *Seuranta ja arviointi*

[48] Valtionvarainministeriö, VAHTI-toiminta verkkosivu.

Kuva 10. Digitaalisen turvallisuuden kehittäminen ja ohjaaminen valtionhallinnossa.[49]

[49] Valtionvarainministeriö, VAHTI-toiminta verkkosivu.

5 POHDINTA

Tässä opinnäytetyössä tutkimuksen kohteena oli EU:n tietosuoja-asetus ja sen määrittelemä tietoturvallisuuden taso ja vaatimukset henkilötietojen turvalliselle käsittelylle. Tutkielman tavoitteena oli tutustua EU:n tietosuoja-asetukseen ja erityisesti sen 32-34 artiklan määritelmiin, sekä alan tunnustettuihin standardeihin kuten ISO/IEC 27000 sekä kotimaiseen VAHTI-ohjeistukseen ja Katakriin. Tutkielmassa keskitytään erityisesti EU:n tietosuoja-asetuksen määrityksiin tekniselle tietoturvallisuudelle, miltä hyvä tekninen ja operatiivinen tietoturva näyttää ja mitkä ovat merkittävimmät muutokset nykyiseen lainsäädäntöön.

Tietotekniikan kehittyminen on mahdollistanut suurten tietomäärien keräämisen, tallentamisen sekä hyödyntämisen ja henkilötiedot ovat kuin polttoainetta uusille digitaalisille palveluille. Uudet trendit kuten palvelupohjaiset pilvi-ratkaisut tai IoT (Internet of Things) valtaavat alaa ja nämä uudet toimintatavat tulevat räjähdysmäisesti kasvattamaan kerättävän datan määrän seuraavien 5-10 vuoden aikana, kun verkkoon kytketään miljardeja uusia laitteita. Nämä uudet mahdollisuudet tuovat mukanaan myös uusia ja suurempia riskejä, mikä tulee edellyttämään entistä suurempia ja kattavampia turvatoimia. Tämän kehityksen suunnan on myös Euroopan Unioni huomannut ja nyt myös reagoinut tämän uuden asetuksen ja direktiivin kautta. Merkittävimmät muutokset suurempien organisaatioiden näkökulmasta tulevat todennäköisesti olemaan velvoite nimittää tietosuojavastaava, joka on puhtaasti uusi henkilöresurssi tai hankittu palvelu. Tämän lisäksi tulee velvollisuus ilmoittaa henkilötietoihin kohdistuneista tietoturvapoikkeamista viranomaisille, jolla saattaa olla merkittävä vaikutus organisaation imagolle sekä viimeisimpänä, mutta ei vähäisimpänä, mahdollista tietomurtoa seuraavat hallinnolliset sanktiot jotka saattavat organisaation liikevaihdosta riippuen nousta useisiin satoihin miljooniin euroihin.

Tämän asetuksen käyttöönotto organisaatioille tuskin tulee olemaan aivan ongelmatonta. Saati sitten hallinnollisten sanktioiden määrääminen mahdollisen tietomurron takia. EU:n tietosuoja-asetus ei itsessään tarkkaan määrittele, mikä on riittävä tekninen ja operatiivinen tietoturvan taso, joten tämä tullaan arvioimaan todennäköisesti tapauskohtaisesti ja tuleekin olemaan mielenkiintoista nähdä ensimmäinen ennakkopäätös, jolla sanktioita rikkomuksesta määrätään. Tämä tulee antamaan suunnan kaikille tuleville tapauksille ja

antaa myös tarkemman kuvauksen EU:n asetuksen edellyttämästä teknisen ja operatiivisen turvallisuuden tasosta. Tällä hetkellä organisaatiot voivat turvautua esimerkiksi yleisesti tunnustettuihin tietoturvallisuusstandardeihin ohjatessaan omaa toimintaansa. Kansainvälisestä näkökulmasta useat suuremmat organisaatiot jotka ovat jo esimerkiksi saavuttaneet ISO/IEC 27001-sertifioinnin ja hyvinkin pitkälti jo täyttävät EU:n tietosuoja-asetuksen edellyttämät vaatimukset. Valitettavasti Suomessa etenemistahti ei ole ollut yhtä hyvä ja SFS ry:n tutkimuksen mukaan vuonna 2014 puhuimme vain kymmenistä organisaatioista, jotka olivat ISO/IEC 27001-sertifikaatin hankkineet. Uskonkin, että seuraavien kuukausien aikana monella organisaatiolla tulee olemaan kiire arvioida omaa tilannettaan ymmärtääkseen millä laajuudella tietosuoja-asetus tulee heitä koskettamaan. Organisaation koosta, toimintatavoista ja toimialasta riippuen muutokset voivat olla merkittäviä ja aikataulu liian tiukka ja käytössä olevat resurssit liian vähäiset.

Tulevaa muutosta kuitenkin voidaan pitää hyvänä, koska kaikki yhteiskunnan palvelut alkavat olla digitaalisessa muodossa ja organisaatioiden toiminta lähes riippuvaista teknologista. Kaikki toiminta tulee perustumaan massiiviseen määrään tietoa, jota kerätään kaikista meistä. Tämä tulee avaamaan uusia rajapintoja esimerkiksi järjestäytyneelle rikollisuudelle ja nostamaan tiedon digitaalisen muotoon kohdistuvat kyberturvallisuuden uhkat aivan uudelle tasolle. Uusi EU:n tietosuoja-asetus ja sen edellyttämät velvoitteet ja mahdolliset seuraamukset velvoitteiden rikkomisesta tuovat mukavasti huomiota näihin tulevaisuuden näkymiin ja uhkiin. Tämä tulee myös pakottamaan organisaatiot miettimään tietoturvaa ja tietosuojaa omassa toiminnassaan sekä rakentamaan riittävät tekniset ja prosessuaaliset keinot tietojen ja toimintansa turvaamiseksi.

LÄHTEET

Andreasson Ari, Koivisto Juha, 2013, Tietoturvaa Toteuttamassa, Tietosanoma Oy

CGI Kyberturvallisuus digitalisoituvassa maailmassa, 2016, https://www.cgi.fi/sites/default/files/files_fi/pdf/whitepaper_kyberturvallisuus-digitalisoituvassa-maailmassa.pdf

CGI Kyberturvallisuuden tila suomalaisissa organisaatioissa, 2016, https://www.cgi.fi/sites/default/files/files_fi/pdf/cgi_kyberturvallisuuden-tila_tutkimuraportti2016.pdf

Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe 2004-2014

Euroopan neuvoston ja parlamentin direktiivi (EU) 2016/1148, http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, EU:n virallinen lehti, 27.4.2016,http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

Hirvonen, Ari, 2011, Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. http://www.helsinki.fi/fi/oikeustieteellinen-tiedekunta/tutkimus

ICC Cyber security guide for business 2015

International Chamber of Commerce (ICC), ICC Cyber security guide for business 2015, https://kauppakamari.fi/wp-content/uploads/2016/11/kyberturvaopas.pdf

ISO/IEC 27000:2016(E), http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Järvinen Petteri, 2010, Yksityisyys – Turvaa digitaalinen kotirauhasi, Saarijärven Offset Oy

Katakri 2015, https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Karvi T, Tietojenkäsittelylaitos, Helsingin Yliopisto, 2011, Tietoturvan perusteet, https://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_11.pdf

Liikenne ja viestintäministeriö, Julkaisuja 4/2016, Maailman luotetuinta digitaalista liiketoimintaa, Työryhmän ehdotus Suomen tietoturvallisuusstrategiaksi, http://urn.fi/URN:ISBN:978-952-243-475-3

NIST Special Publication 800-33, National Institute of Standards and Technology, 2001 http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

Nyyssölä Mikko, Alma Talent Oy. 2014. Yksityisyyden suoja työsuhteessa.

EU:n yleisen tietosuoja-asetuksen (2016/679) valmistelun vaiheet. 2017. OpiTietosuojaa verkkodokumentti. https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-%20tietosuoja-asetus/23-tuleva-eu-n-tietosuoja-asetus

Pitkänen Olli, Tiilikka Päivi ja Warma Eija. 2013. Henkilötietojen suoja, Alma Talent Oy ja tekijät

Ponemon Institute, Cost of Data Breach Study, 2015, https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF

Suomen Standardisoimisliitto SFS ry, 2015, ISO/IEC 27000:2015 Kalvosarja oppilaitoksille. http://SFSEdu.fi

Tietosuojavaltuutetun toimiston lehdistötiedote 10.10.2012 http://www.tietosuoja.fi/59848.html

Thomas Tom, 2004, Verkkojen Tietoturva, Edita Publishing Oy

VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus, https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

VAHTI-Tietoturvapoikkeamatilanteiden hallinta, 2017, Valtionvarainministeriön julkaisuja 8/2017. https://julkaisut.valtioneuvosto.fi/handle/10024/79258

VAHTI, Kimmo Rousku, Valtionvarainministeriön julkaisuja 25/2017, Sähköisen asioinnin tietoturvallisuusohje, http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80012/VM_25_2017.pdf?sequence=1

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010. http://www.finlex.fi/fi/laki/alkup/2010/20100681

Valtionvarainministeriö, VAHTI-toiminnan verkkosivut, http://vm.fi/vahti

Viestintävirasto, Viestintäviraston julkaisu 001/2017 J, Tietoturvan vuosi 2016, https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf